A Companion to
User's Guide to Cryptography and Standards

Alexander W. Dent   Chris J. Mitchell

17th December 2004 (v1.1)

Contents

Preface

Preface to version 1.0

This companion is intended to supplement and update the *User's Guide to Cryptography and Standards*. Such is the speed at which standards evolve that the User's Guide is, unfortunately, already out of date at the time of writing, and it has only just appeared in print. Our plan is to regularly update this companion so that, in conjunction with the User's Guide itself, the reader is given information that is as current as we can make it.

The structure of this companion is identical to that of the User's Guide. All the end of chapter notes, the complete appendix, and the entire list of references are reproduced from the User's Guide, updated where appropriate. The text from the main body of each chapter is not reproduced, although the headings have been retained; text is included under the original headings where the status of the subject has changed (or it seems appropriate to provide additional information).

As always, we would very much welcome input of all kinds on the User's Guide and this companion. We would particularly welcome corrections and additions to the existing text, which we will do our best to acknowledge.

<div align="right">

Alex Dent
Chris Mitchell
November 2004.

</div>

Chapter 1

Introduction

1.1   Scope and purpose

1.2   Structure of book

1.3   Terminology

1.4   Modular Arithmetic

1.5   Notes

§1.1

There are many useful books on cryptography — we mention just three. Murphy and Piper's book [470] provides a very simple introduction to cryptography. Schneier's book [496] is a very readable account of modern cryptography. In the notes in subsequent chapters we refer to books containing more detail on the topics covered in the particular chapter. Of particular importance in this respect is the Handbook of Applied Cryptography, [407], which provides a detailed and meticulously researched account of cryptographic topics.

It is interesting to note that both modern cryptography and information theory owe a huge debt to the pioneering work of Shannon, who published enormously influential papers on both topics in the post-war years [500, 501].

§1.4

There are many books providing simple explanations of modular arithmetic and related concepts. Indeed, almost any book on modern cryptography will provide an explanation. Chapter 2 of the Handbook of Applied Cryptography [407] provides an extremely useful introduction to not only modular arithmetic but also many other mathematical concepts necessary to understand modern cryptography.

Chapter 2

Standards and the standardisation process

2.1   Why bother with standards?

2.2   International standardisation organisations

2.3   National standardisation organisations

2.4   Industrial standardisation organisations

2.5   Cryptographic evaluation bodies

2.6   Notes

There are thousands of standards on a huge range of different topics (as a quick look on the ISO website will confirm) and all of them are designed to specify a common method of doing a routine task. The eight reasons for standardisation given by the BSI and discussed in Section 2.1 are taken from the BSI website. A history of the ISO standardisation body is available on the ISO website:

        http://www.iso.ch/iso/en/aboutiso/introduction/fifty/fifty.html

Several standards are mentioned during the discussion of standardisation bodies: these will be discussed in detail later in the book. SEC 1 [510] and SEC 2 [511] will be discussed in Chapter 4; ISO 8370 [230] and ISO 8371 [225, 235] will be discussed in Chapter 7; ISO/IEC TR 14516 [296] will be discussed in Chapter 14; ISO/IEC WD 19790 [322], ISO/IEC CD 18031 [309] and BS 7799 [94, 95] will be discussed in Chapter 16.

The sister organisation to IETF, the Internet Research Task Force (IRTF), is also involved with cryptography. The IRTF conducts its research by creating small research groups to work on topics related to the Internet, and one such research group, the Crypto Forum Research Group (CFRG), is focused on cryptography. More information about the IRTF can be found at:

                        http://www.irtf.org/

whilst information about the CFRG can be found on its homepage:

                        http://www.irtf.org/cfrg/ .

For more information about the IETF and its standardisation efforts, the reader is referred to two of the IETF's own documents: RFC 1118 [378] and RFC 2026 [89]. For more general information on standardisation, Chapter 15 of Menezes, van Oorschot and Vanstone [407] and the appendices of Ford [170] both contain introductions to the subject.

Chapter 3

Security mechanisms and security services

3.1   Introduction

3.2   Security standards

3.3   A model for security

3.4   Security services

3.5   Security mechanisms

3.6   Relating services to mechanisms

3.7   Services and protocols layers

3.8   Security management

3.9   Security frameworks

3.10   Notes

§3.1

The OSI model is specified in ISO/IEC 7498-1, the second edition of which was published in 1994 [241].

Ford's book [170] provides an excellent standards-based introduction to network security that is essentially complementary to the scope of this book. Section 1.2 of the Handbook of Applied Cryptography [407] and the foreword to [505] also provide brief introductions to security services and mechanisms.

§3.2

ISO 7498-2 [227] was published in 1989 as one part of the OSI 'basic reference model', and a version of this document was also adopted as CCITT Recommendation X.800 in 1991 [323] (an amendment to this latter recommendation, addressing LAN security issues, was published in 1996 [333]).

The seven part ISO/IEC security frameworks standard, ISO/IEC 10181, was published in 1996/97 [248, 249, 250, 251, 252, 253, 257]. The identical ITU-T recommendations, X.810–X816, were published a little earlier [327, 328, 329, 330, 331, 332, 334].

ISO/IEC TR 13594 [247], the lower layers security model, (see also X.802 [326]) and the upper layers security model ISO/IEC 10745 [245] (see also X.803 [325]) are not

discussed in detail here. However Ford [170] provides a comprehensive description of lower and upper layer security.

The ITU-T security architecture for end-to-end systems, i.e. X.805, was published in 2003 [347].

ISO/IEC 15816, standardising security labels, was published in 2001 [288], and the identical ITU-T recommendation, X.841, was published a few months earlier, [337].

§3.3

The CRAMM risk assessment methodology originated from a UK government initiative, but today is a commercial product. For more information about CRAMM see

```
http://www.cramm.com
```

§3.4

The discussion of security services in this chapter is very much oriented towards communications security issues. This contrasts with the common division of security services into Confidentiality, Integrity and Availability (CIA) in a computer security context. For more details of this approach see, for example, Chapter 1 of Gollmann [187] or Chapter 1 of Pfleeger [467].

The division of non-repudiation into two sub-services contrasts with the approach in ISO/IEC 13888-1 (see Chapter 9), where a total of eight non-repudiation services are defined.

A description of LAN protocols, X.25 PSNs, IP and TCP can be found in just about any book on computer networking; see, for example, Stallings [509].

§3.5

Defining encryption mechanisms to be a special case of encipherment mechanisms, and defining hash-functions as a separate class of encipherment mechanisms, departs somewhat from common use of these terms. Indeed, most cryptographers would equate encipherment and encryption, and would regard hash-functions as being something else entirely. The reason we have departed from the commonly used terminology is that the usage here would appear to be the only way to apply the ISO 7498-2 classification of mechanisms without making major modifications to it.

Although access control mechanisms are not discussed in this book, they are extremely important and have been the focus of a huge amount of research effort. For further details of some of this work see Bishop [63] or Ferraiolo, Kuhn and Chandramouli [167].

ISO/IEC TR 15947 [297] provides a framework for intrusion detection systems; intrusion detection is also the focus of the IETF `idwg` working group (the Intrusion Detection Exchange Format working group).

§3.6

For further information about OSI see, for example, Henshall and Shaw's book [205], and for a review in the context of security issues see Ford [170].

§3.7

Firewalls are a very widely used type of network security device. Books on firewalls include those of Cheswick, Bellovin and Rubin [111] and Zwicky, Chapman and Cooper [533].

The description of the Internet protocol hierarchy is based on Ford [170]. In fact, this protocol hierarchy is described in just about any modern book on computer networking (see, for example, [509]).

§3.8

The OSI management framework, ISO/IEC 7498-4 [228], was published in 1989.

The US DoD 'Orange Book' [136], published in 1985, was the first standard for security system evaluation. More recently, the internationally harmonised 'Common Criteria' have been developed and standardised in ISO/IEC 15408, parts 1–3 [273, 274, 275]. There are many books describing the various evaluation criteria. Ford [170] provides an introduction, as does Gollmann [187].

§3.9

Chapter 6 (pages 149-176) of Ford's book [170] is relevant to the discussion of the access control framework. Many of the ideas in the access control framework come in fact from earlier pre-standardisation efforts by ECMA [151].

Chapter 4

Encryption

4.1   Definitions and Basic Properties

4.2   Block Ciphers

In July 2004, NIST announced its intention to withdraw its support for the DES block cipher and asked for comments. The proposed withdrawal would affect both NIST FIPS 46-3 (the specification of DES and triple DES) and NIST FIPS 81 (the modes of operation for DES — see Chapter 5). NIST would continue supporting the use of Triple DES through the publication of a Special Publication: NIST SP 800-67. Despite this continued support for Triple DES, the withdrawal announcement makes it clear that NIST would prefer all cryptographic applications requiring a block cipher to use the new AES.

ISO/IEC 18033-3 on block ciphers is now nearing completion (the current version is the Final CD), and the selection of block ciphers included in this draft standard appears to have stabilised. FCD 18033-3 contains a total of six block ciphers, split into two categories. The are three 64-bit ciphers (Triple DES (called TDEA), MISTY1 and CAST-128), and there are three 128-bit ciphers (AES, Camellia and SEED).

4.3   Stream Ciphers

Part 4 of ISO/IEC 18033 on stream ciphers is also now nearing completion (the current version is the Final CD), and apart from the CFB, OFB and CTR modes of operation of a block cipher, contains two 'dedicated' keystream generators for synchronous stream ciphers. These are the MUGI and SNOW 2.0 schemes.

Bluetooth

One important "dedicated" stream cipher in practical use is the Bluetooth keystream generator, produced by the Bluetooth SIG (Special Interest Group). The Bluetooth SIG produce specifications to allow mobile devices (such as cellular phones, PDAs and laptops) to communicate securely through device-to-device wireless links. The stream cipher specification, known as E0, is designed to provide confidentiality for this link. Unfortunately, several attacks against this stream cipher have been proposed and the Bluetooth SIG are currently discussing a replacement for E0.

4.4 Asymmetric Ciphers

Like the other parts of ISO/IEC 18033, Part 2 on asymmetric ciphers is now nearing completion (the current version is the Final CD), and the selection of ciphers included in this draft standard appears to have stabilised. The six selected algorithms can be divided into three categories:

- ElGamal-based schemes (ECIES-KEM, PSEC-KEM, ACE-KEM)

- RSA-based schemes (RSA-OAEP, RSA-KEM)

- Rabin-based schemes (HIME-(R))

4.5 Notes

§4.1

This chapter is only meant to act as an introduction to the world of encryption, not as an exhaustive study of the subject. In terms of the study of standardisation, very little is actually gained by describing the actual encryption schemes that we have discussed — their design methodologies are not easily understood and detailed descriptions of the algorithms are remarkably unenlightening on their own.

Semantic security was formally introduced by Goldwasser and Micali [182] and studied further by Micali, Rackoff and Sloan [414]. The more modern notions of security for symmetric and asymmetric ciphers, and the relationships between these notions, are discussed in two excellent papers: one on symmetric ciphers [46] and one on asymmetric ciphers [47].

The reader who is looking for a more comprehensive academic treatment of encryption schemes is referred to one of the many introductory books on the subject [178, 179, 470, 496, 513, 521]. An algorithmic description of many cryptographic algorithms discussed in this chapter can be found in Menezes, van Oorschot and Vanstone [407].

§4.2.1

The latest version of the Data Encryption Standard is contained in NIST FIPS Pub. 46-3 [441] and the corresponding ANSI standard [34]. These documents standardise both the original version and the Triple-DES variant, although the original version is not actually recommended for use as a confidentiality algorithm. Triple-DES is also standardised in the draft ISO/IEC 18033-3 standard [300].

In July 2004, NIST asked for comments regarding a proposed withdrawal of DES [452]. The proposal would remove NIST's support for the DES algorithm by withdrawing NIST FIPS 46-3 [441] and NIST FIPS 81 [437]. Support for Triple DES would be provided via a Special Publication: NIST SP 800-67 [453].

Details of the exhaustive key search performed by Curtin and Dolske can be found in [125].

The idea of building a dedicated machine for cracking DES by exhaustively searching through all possible keys — a DES cracker — was first suggested by Wiener [523]. The Electronic Frontier Foundation, the organisation that practically demonstrated the practical weakness of 56-bit DES keys so effectively by building the DES cracker, is contactable through its website

$$\texttt{http://www.eff.org/}$$

and details about the DES cracker in particular can be found at

$$\texttt{http://www.eff.org/descracker}\ .$$

The existence of the DES cracker has put the final nail in the coffin of DES. It is interesting that it is the short key, an issue which was brought up during the standardisation process itself, rather than any later cryptographic developments, which has caused the cipher to fall.

The two greatest developments in the cryptanalysis of block ciphers were the discovery of differential and linear cryptanalysis. Differential cryptanalysis was introduced into the public domain by Biham and Shamir [60], although their work is similar to an unpublished attack against DES by Davies (later published by Davies and Murphy [132]). Biham and Shamir went on to use differential cryptanalysis to break DES [61] even though it seems as if one of the design conditions for the cipher was its resistance to exactly this kind of cryptanalysis. Linear cryptanalysis was introduced by Matsui [398] and has also been applied to DES.

§4.2.2

The ISO register of cryptographic algorithms can be found on the Internet at

$$\texttt{http://www.iso-register.com/}\ .$$

The register is currently maintained by Royal Holloway on behalf of the BSI and ISO. The procedures for registering a cryptographic algorithm are given in ISO/IEC 9979 [280].

The block cipher IDEA [407] was one of the original choices for use with the PGP e-mail encryption system and is the subject of a Swiss National Standard. The block cipher MISTY1 [399] is the primary recommendation of the NESSIE algorithm analysis project for a 64-bit block cipher and is contained in an IETF RFC [461]. Both algorithms have been proposed (along with Triple-DES) for inclusion in the ISO encryption standard [300].

For more information on the history and politics of cryptography, the reader is referred to Diffie and Landau [140] and Hoffman [208].

§4.2.3

The AES is available as NIST FIPS Pub. 197 [444]. It is the primary recommendation of the NESSIE algorithm analysis project for a 128-bit block cipher. It appears that the main reasons why Rijndael was selected as the AES are its flexibility and

its efficiency on a wide variety of software and hardware platforms — it is especially well designed for use with smart cards, for example. A good overview of the AES standardisation process is given in Burr [99] and Danielyan [128].

However, a number of recent papers have demonstrated some interesting and unusual properties of Rijndael. The most of interesting of these are by Courtois and Pieprzyk [124] and Murphy and Robshaw [432]. Both of these rely on the fact that the inner structure of the AES can be easily represented as a simple algebraic structure – thus giving rise to a description of the cipher as a series of simple, low-degree algebraic equations. Whether these properties will give rise to practical attacks against the AES is not yet known, however this does not seem to be stopping the standardisation or implementation of the cipher.

Despite these unusual properties, AES has been approved by the U.S. government to protect confidential information [118].

§4.2.4

The criteria for the cryptographic algorithms used in third generation mobile phones were first set down in June 1999 [153]. Since then they have been updated several times, the latest version having been released in July 2001.

The cryptographic algorithm requirements do not specifically mention the need for a block cipher, but only specify the properties that the confidentiality and integrity functions $f8$ and $f9$ should have. It is the specification of $f8$ and $f9$ [154] that contains the first explicit references to the KASUMI block cipher [155].

§4.2.5

The general guidelines for the selection of encryption algorithms for standardisation by ISO is given in ISO/IEC 18033-1, currently out for FDIS ballot [317]. The part of ISO/IEC 18033 concerning block ciphers is Part 3 [313], which is currently at the FCD stage. Of the six schemes in FCD 18033-3, AES, MISTY1 and triple DES have already been discussed; Camellia [38] is rather similar to AES; CAST-128 [19] is a Canadian national standard; and SEED [514] is a Korean national standard.

§4.3

The A5/1 and A5/2 stream ciphers were also reverse engineered by Briceno, Goldberg and Wagner [92] and have been attacked by numerous authors, the most recent and damning of which is by Barkan, Biham and Keller [42]. This final attack is pretty devastating, recovering the secret key relatively quickly by observing encrypted ciphertexts as they are transmitted. The A5/3 stream cipher [162] has not yet been broken.

There are no known weaknesses in the third generation confidentiality algorithm, $f8$ [154].

The general model for a stream cipher is adapted from ISO/IEC FCD 18033-4 [314]. More information on the history and properties of the CFB, OFB and CTR modes of operation for a block cipher can be found in Chapter 5. Both the MUGI [520] and SNOW 2.0 [149] schemes were published as recently as 2002. Whilst some

preliminary analysis of both these schemes has been performed [184, 519], there are no known serious weaknesses of these schemes.

The Bluetooth stream cipher E0 [75] has been the subject of many proposed attacks [169, 185, 206, 354, 395] and the Bluetooth SIG are currently discussing replacements for this algorithm.

§4.4

Whilst the first encryption scheme was the hugely successful RSA scheme, introduced in 1978 [484], the first probabilistic encryption scheme was introduced by Goldwasser and Micali [182] in 1984. Today almost all proposed asymmetric encryption schemes are probabilistic because it has been found that deterministic schemes cannot meet the high security criteria demanded of modern ciphers (i.e. deterministic schemes cannot be semantically secure). More information about the security requirements for modern asymmetric ciphers can be found in [47].

§4.4.1

The first asymmetric algorithm (and the introduction of the concept of asymmetric algorithms) was given in a paper by Diffie and Hellman [138]. This paper contain the Diffie-Hellman key agreement protocol but stopped short of giving an encryption scheme. The first asymmetric encryption scheme was given by Rivest, Shamir and Adleman [484]. Since its inception, numerous attacks have been made against the RSA cipher but none of them have proved enough to break the scheme completely. There are, however, too many to detail here. A good survey of attacks against RSA can be found in [83].

§4.4.2

Both the RSA PKCS and the SECG standards are freely available on the Internet (see Chapter 2 for more information about obtaining standards). The most famous attack against RSA PKCS was by Bleichenbacher [73] and attacked not the RSA scheme itself but the padding system used to format messages before they were encrypted using RSA. After the initial efforts of the SECG, elliptic curve cryptography has been quickly accepted by both cryptographers and implementors. It is now also standardised by the IEEE 1363 group [221, 223], ISO/IEC JTC1 [292] and is now even being included in the RSA PKCS. A good introduction to elliptic curve cryptography is given by Hankerson, Menezes and Vanstone [202]. More technical issues associated with elliptic curves are discussed in Blake, Seroussi and Smart [68, 69].

§4.4.3

Two IEEE standards have been published [221, 223] and two more are in development. Of the two standards in development, only the draft standard on lattice based techniques proposes any kind of encryption scheme.

Lattice based cryptography seems to have been developed in a rather bizarre fashion. Initially lattices were only used as a tool for attacking certain types of cryptosystem (particularly "knapsack" cryptosystems, see [521]). It wasn't until the

NTRU public-key cryptosystem was proposed during the rump session of the Crypto '96 conference that it was considered a viable basis for a cryptographic scheme. The NTRU encryption scheme was shown to be equivalent to a particular lattice problem [122] and it seems that, for suitably chosen parameters, this problem would be hard to solve – thus showing the security of the cryptosystem. Despite this 'security proof', there have been many problems with NTRU and it has not yet been fully accepted by the cryptographic community. Other lattice schemes have since been proposed, for example [180] proposed by IBM Research, but have similarly failed to be universally accepted.

As we have stated, one of the main strengths of lattice based cryptography is that it seems to be resistent to attacks made by quantum computers. Quantum computing is a vastly complex subject that takes in elements of mathematics, atomic physics and cryptography, and is far beyond the scope of this book. It is known, however, that a quantum computer would be able to efficiently break both the RSA and the Diffie-Hellman schemes [503]. For more information the reader is referred to [459].

§4.4.4

The ISO standard on asymmetric encryption (ISO/IEC FCD 18033-2 [312]) is the first to so fully embrace the use of hybrid ciphers. Of the six algorithms proposed for inclusion only two are not hybrid ciphers, and the four hybrid ciphers that are proposed are KEM/DEM constructions. The idea of a hybrid asymmetric encryption scheme has been "cryptographic folklore" for years and almost all practical uses of asymmetric encryption involve hybrid schemes (including the PGP encryption scheme, SSL/TLS encryption and IPSec). However, the idea has only recently been formalised [504].

Whilst a KEM/DEM construction is far from being the only way in which one can construct a hybrid cipher, it does have certain attractive security features. It now appears likely that the ISO/IEC standard will contain at least one KEM based on RSA (RSA-KEM) and at least one KEM based on the Diffie-Hellman key agreement protocol (ECIES-KEM and/or PSEC-KEM). PSEC-KEM was the primary choice of the NESSIE evaluation project for an asymmetric encryption scheme.

Chapter 5

Modes of operation for block ciphers

5.1   Definitions and basic properties

5.2   Standards for modes of operation

5.3   Padding methods

5.4   Electronic Codebook (ECB) mode

5.5   Cipher Block Chaining (CBC) mode

5.6   Counter (CTR) mode

5.7   Output Feedback (OFB) mode

5.8   Cipher Feedback (CFB) mode

5.9   Choosing a mode of operation

5.10   Other modes

5.11   Notes

§5.1

For a more detailed treatment of modes of operation for block ciphers, the reader is referred to Chapter 7 of the Handbook of Applied Cryptography [407].

§5.2

The original NBS FIPS on block cipher modes of operation [437] was published in 1980, and ANSI X3.106 [33] followed in 1983. The ISO 64-bit modes of operation standard ISO 8372 (now withdrawn), based very closely on ANSI X3.106, appeared in 1987 [224]. The n-bit version of this latter standard, namely ISO/IEC 10116, has been through three revisions [232, 256, 311].

The most recent (3rd) edition of ISO/IEC 10116 [311], due to be published in late 2004 or 2005, contains the CTR mode (first proposed by Diffie and Hellman in 1979 [139]), which is also contained in NIST Special Publication 800-38A [447]. An overview of the NIST standardisation effort that led to NIST Special Publication 800-38A can be found in [99].

The 3GPP standard 3GPP TS 35.201 [154] contains a modified version of OFB mode.

§5.3

Vaudenay [517] pointed out the possibility of attacks on messages encrypted using CBC mode in a special scenario where an attacker can modify messages and send them to the authorised decryptor, and then observe error messages indicating padding format failures in decrypted messages. In such a case an attacker can, by repeating this process, learn information about the plaintext. This attack takes advantage of a particular choice for a padding method. Black and Urtubia [67] and Paterson and Yau [465] have extended this attack to other padding techniques, and Canvel et al. [106] have provided a practical demonstration of the attack. These attacks show that it is important that the padding method is selected appropriately, and for error messages to be handled with great care. As argued by Black and Urtubia, the existence of such attacks argues strongly in favour of the use of authenticated encryption modes (see Section 5.10 and Chapter 16) wherever possible.

§5.4

The ECB mode should not be used even for short messages unless the data being encrypted is highly random or unless a single key is only used to encrypt a small number of blocks. To see why, suppose a 64-bit block cipher is used to encrypt single blocks, each made up of eight letters. There will thus be only $26^8 \simeq 2 \times 10^{11}$ possible different plaintext blocks, and hence the same block is likely to occur twice after only around $26^4 \simeq 500,000$ plaintext blocks have been encrypted.

§5.5

A 'proof of security' for the CBC mode was published by Bellare et al. in 1997 [46]. This proof requires the Starting Variable to be a secret (known only to the legitimate sender and receiver).

The modification to CBC mode known as ciphertext stealing is due to Meyer and Matyas [412]. Mitchell and Varadharajan [427] pointed out the hazards of using OFB mode to encrypt the final block.

§5.6

A formal treatment of CTR mode has been presented by Bellare et al. in [46].

§5.7

The probability of the same sequence of bits being used to encrypt two different messages can be reduced by not 'restarting' OFB every time a message is encrypted. That is, after encrypting a message, the encrypter stores the final value of X_i to be used as the Starting Variable for the next message. However, even with this approach, a single key should not be used to encrypt more than $\sqrt{2^n}$ blocks for the following reason. Knowledge that the keystream will, with high probability, not repeat leaks information about the plaintext (see Bellare et al. [46]).

A 'proof of security' for the version of OFB contained in the 3GPP standard [154], was published by Kang et al. in 2001 [365]. However, this proof was shown to be incorrect by Iwata and Kurosawa in 2003 [350], although this does not mean that any significant weakness has been found in this function. Indeed, by making a slightly stronger assumption about the security of the block cipher, Iwata and Kohno [348] have recently provided a new proof of security for this modified OFB mode.

§5.8

The CFB mode is an example of what is known as a 'self-sychronising stream cipher'; such systems have a long history (see also Chapter 4). In fact a version of CFB mode was first proposed by Diffie and Hellman in 1979 [139]. If used with $j = 1$, then this technique will, after a delay, recover from all types of errors, including insertion or deletion of bits (see Chapter 6 of [407]).

§5.9

Error propagation is probably only desirable if data integrity and data origin authentication services are to be based on a combination of encryption and the addition of redundancy. Unfortunately, none of the known constructions of this type, i.e. which simply involve adding redundancy to data prior to applying encryption using one of the standard modes, satisfy any of the reasonable security definitions (see, for example, [36, 367]). Reliably achieving confidentiality and integrity would appear to require a somewhat more sophisticated approach, e.g. as provided by the authenticated-encryption modes (briefly discussed in Section 5.10.2).

§5.10

Prior to the publication of ANSI X9.52 in 1998 [28], various other modes of operation specifically designed for use with triple DES had been proposed, and some of them appeared in draft versions of this standard. One of them, known as CBCM, was shown to be weak by Biham and Knudsen [58, 59], and was removed from the published standard.

The first working draft of ISO/IEC 19772 appeared in early 2004 [321]. The OCB mode was originally proposed by Rogaway, Bellare and Black [486]. The CCM mode is contained in RFC 3610 [522] and NIST special publication 800-38C [451], a draft NIST recommendation for an authenticated encryption mode. AES key wrap is specified in Internet RFC 3394 [495].

Chapter 6

Cryptographic hash-functions

6.1 Definitions and Basic Properties

6.2 Standards for Hash Functions

6.3 Hash Functions Based on Block Ciphers

6.4 Dedicated Hash Functions

6.5 Hash Functions Based on Modular Arithmetic

6.6 Choosing a Hash Function

6.7 Notes

§6.1

Many people have tried to define the properties that a hash function must have in order to be secure. These definitions are usually sufficient for most uses of a hash function but, almost always, the definitions are not sufficient for some small set of anomalous cases. The properties of 1st and 2nd pre-image resistance, and collision resistance are the normal benchmark levels of security for a hash function. The notions of 1st and 2nd pre-image resistance were first noted by Merkle [408, 409]. Collision resistance was introduced by Damgård [126].

Most hash functions that are 2nd pre-image resistant (or collision resistant) are also 1st pre-image resistant but this is not necessarily the case. A good example of a collision resistant hash function that is not pre-image resistant can be found in Menezes, van Oorschot and Vanstone[407]. Suppose g is a collision resistant hash function that produces outputs of length k (in bits). We can define a new hash function h by setting

$$h(x) = \left\{ \begin{array}{ll} 1||x & \text{if } |x| = k\,, \\ 0||g(x) & \text{otherwise}\,. \end{array} \right. \tag{6.1}$$

This hash function is clearly not pre-image resistant. However, in order to find a collision in this hash function we need to find a collision in the hash function g and we have already stated that g is a collision resistant hash function. Hence h is a collision resistant hash function that is not pre-image resistant. The relationship between the different notions of security for a hash function are explored in [488].

In a significant proportion of cases, however, more is demanded from a hash function then the three standard properties of 1st pre-image resistance, 2nd pre-image resistance and collision resistance. In many cases it is assumed that a hash function will behave like a random function. This is especially true when analysing the security of asymmetric algorithms, where this randomness assumption is known as the random oracle model [50]. The concept that a function could be indistinguishable

from a random function was first suggested by Goldreich, Goldwasser and Micali [181]; however unkeyed hash functions cannot be indistinguishable from a random function. Nevertheless, where hash functions are used in complex algorithms, it is often assumed that unkeyed hash functions behave randomly in order to simplify the security analysis.

The first examples of an iterative hash function appeared in the late 1970s [408, 478]. The modern general model is more closely aligned to the "Merkle meta-function" proposed by Merkle [410, 411] and Damgård [127]. The construction by Merkle seems to be the first to suggest that some form length parameter should be included in the input to the round function (see padding method 3 in Section 6.3.1). This helps to prevent certain attacks.

However, in 2004, Joux [358] gave an example of a type of attack that was enabled by the iterative nature of modern hash function design. The attack shows that, in certain constructions, it is easier to find collisions in iterative hash functions than in random functions. It is unclear whether this will lead to a re-evaluation of the iterative method of designing hash functions.

It can be argued that a hash function can provide a certain set of limited security services on its own. For example, the hash of a message can be printed out and stored in a physically secure device, such as a safe. A user can then check the integrity of the message at a later date. Alternatively a message could be sent over one channel and the hash of the message sent over a second, again to ensure message integrity. In essence, a hash function can reduce the problem of message integrity from the need to protect the integrity of a long data string to the need to just protect the integrity of a short hash-code.

As always, descriptions of most of the hash functions discussed in this chapter can be found in Menezes, van Oorschot and Vanstone [407].

§6.2

The major standards for hash functions are:

- ISO/IEC 10118-1 [282] (General information about hash functions),
- ISO/IEC 10118-2 [283] (Hash functions using an n-bit block cipher),
- ISO/IEC 10118-3 [303] (Dedicated hash functions),
- ISO/IEC 10118-4 [262] (Hash functions using modular arithmetic),
- NIST FIPS Pub. 180-2 [448] (The SHA family of dedicated hash functions),
- IETF RFC 1319 [362] (MD2),
- IETF RFC 1320 [482] (MD4),
- IETF RFC 1321 [483] (MD5),
- IETF RFC 3174 [146] (SHA-1).

§6.3

Block cipher hash function 1 was invented by Matyas, Meyer and Oseas [403] in 1985. Block cipher based hash functions whose hash code is the same size as the block length have been systematically researched by Preneel, Govaerts and Vandewalle [474]. Their conclusion is that the Matyas, Meyer and Oseas scheme is one of a class of only 12 secure block cipher based hash functions. Block cipher hash function 2, also known as MDC-2, was proposed by Matyas, Meyer and Schilling [402, 413]. It is the subject of an IBM patent (U.S. Patent Number 4,908,861).

For block cipher based hash function 1, the function u that derives a block cipher key from an intermediate value is completely specified by the standard for the case when the underlying block cipher is DES. One of the roles of this function in the case when the underlying block cipher is DES is to prevent 'weak' DES keys [130] from being used. The use of weak DES keys leads to a trivial attack against the scheme.

The birthday paradox is so named because of the phenomenon that in a group of only 23 people it is more likely than not that two people will share the same birthday. The idea behind this seemingly illogical fact can also be applied to hash functions and MACs (see Chapter 7). It turns out that if a hash function has an output of length n then, despite their being 2^n possible outputs for the hash function, we would expect to find two inputs that have the same hash code after trying $\sqrt{2^n} = 2^{n/2}$ different inputs. Therefore, since block cipher hash function 1 and block cipher hash function 2 have maximum outputs of size n and $2n$ respectively, we would expect to find collisions in these hash functions purely by chance after $2^{n/2}$ and 2^n trials respectively.

In fact, for block cipher hash function 1, there is an even stronger result. It has been shown [66, 474] that if we assume that the underlying block cipher is in some sense 'perfect' then the best possible attack against block cipher hash function 1 is the birthday attack given above.

§6.4

Most dedicated hash functions seem to have been developed as a result of standards initiatives or focused research projects: the SHA family of hash functions were developed for the NIST secure hash standard [448], the RIPEMD family of hash functions was developed by several members of the RIPE project [85], and WHIRLPOOL was developed for evaluation by the NESSIE project [456, 457].

Many of the standardised dedicated hash functions, including four of the five SHA variants and WHIRLPOOL, have recently been analysed by the NESSIE project. The final security report [456] found no major weaknesses in any of these hash functions. The NESSIE project also conducted extensive performance tests for these hash functions on multiple platforms [457].

All of the MDx algorithms were designed by Rivest [362, 482, 483], although the IETF RFC for MD2 was submitted by Kaliski. MD4 was broken outright by Dobbertin [142] who managed to show that the hash function was not collision resistant. Neither MD2 and MD5 have been broken outright yet but in both cases it has been shown that the round functions are not collision resistant [134, 143, 490]. This means that it is possible to find distinct intermediate hash variables H, H' and data input blocks D, D' such that $\phi(D, H) = \phi(D', H')$. This is not the same as being able to find collisions in the complete hash function but it is a good first step.

In fact, the attack against MD2 is even stronger — it has been shown that collisions could be found in the complete MD2 hash function were it not for a checksum block which is added to the input as part of the padding [490].

Subsequently it has been shown that MD2 is not even a pre-image resistant hash function [431].

The security of all of these algorithms was called into question during the Crypto 2004 conference. A paper by Biham and Chen [57] demonstrated new techniques for finding inputs to the SHA-0 hash function (a precursor to the SHA-1 hash function) whose hash codes are "close". A similar method, apparently independently discovered, was proposed by Wang *et al.* for finding collisions in MD4, MD5 and the RIPEMD hash functions [518]. (The RIPEMD hash function is a pre-cursor to the standardised RIPEMD-128 and RIPEMD-160 hash functions.) It is not currently thought that the SHA family of hash functions or WHIRLPOOL are like to be broken in the near future, nor does the existence of attacks that find a collision in a hash function necessarily mean that hash function is completely useless — for example, it is not currently thought that the popular MAC based on the HMAC construction (see Section 7) using MD5 is broken. Prudence, however, suggests that the use of these algorithms is phased out.

§6.5

The MASH family of hash functions was developed through a long series of papers that broke previous schemes and then proposed repairs. A survey of the early work on the MASH family can be found in [175]. The MASH family of hash functions would probably be of most use in a situation where dedicated hardware for modular arithmetic exists, and in particular when this dedicated hardware exists but the remaining computing power is limited.

Chapter 7

Message Authentication Codes (MACs)

7.1   Definitions and basic properties

7.2   Standards for MACs

7.3   CBC-MACs

7.4   MACs based on hash-functions

7.5   Other MAC functions

7.6   Notes

§7.1

For a more general treatment of MACs the reader is encouraged to refer to Section 9.5 of [407]. Properties required of a MAC algorithm are specified in ISO/IEC 9797-1 [276]. The known-key one-wayness property is required in some applications of MAC functions; see, for example, ISO 15764 [302].

§7.2

The idea of computing a CBC-MAC using DES as the block cipher is now over 25 years old [104]. The first standardised MAC technique is SMAC, discussed in Appendix F of the 1980 US Federal Standard FIPS Pub. 81 [437]. This was followed in the early 1980s by two US Banking Standards, ANSI X9.9 [2] and ANSI X9.19 [1] (the first of which was withdrawn in 1999 [29]). The subsequent ISO banking standards include ISO 8730 [230], ISO 8731 Parts 1 and 2 [225, 235], and ISO 9807 [231]. ISO/IEC 9797-1 [276] is in fact the third version of the ISO/IEC CBC-MAC standard — previous editions were published in 1989 [229] and 1994 [242]. Work started on another revision of ISO/IEC 9797-1 in late 2003; the new version will exclude MAC algorithms 5 and 6 and will include OMAC.

Other CBC-MAC schemes include the 3GPP-MAC scheme [154]. RMAC was proposed in 2002 by Jaulmes, Joux and Valette [356] and was then included in a NIST draft [450]. TMAC and OMAC were proposed by Iwata and Kurosawa [349, 379], and are derived from a scheme known as XCBC (due to Black and Rogaway [64]).

HMAC was originally proposed by Bellare, Canetti and Krawczyk [44], before its adoption by the IETF in 1997 [377]. To assist implementors, a set of test vectors for HMAC when used with the hash-functions MD5 and SHA-1 was published in RFC 2202 [109]. ISO/IEC 9797-2, which also incorporates HMAC, was first published in 2000 [286] (like ISO/IEC 9797-1, it includes test vectors for all the standardised MAC algorithms). The US banking standard ANSI X9.71 [11] also adopts HMAC.

§7.3

Internal collision-based attacks against ARMAC were described by Preneel and van Oorschot [477] and Knudsen and Preneel [373]. These attacks motivated the design of MacDES, which was proposed by Knudsen and Preneel [373] as a superior alternative to ARMAC for use with 'weak' block ciphers such as DES. Subsequently, Coppersmith, Knudsen and Mitchell [120, 121], found attacks which, whilst not breaking the scheme in practice, showed that the advantages of MacDES over AR-MAC are not as great as previously thought, although they are still significant.

The 3GPP-MAC scheme was designed specifically for use with the 3GPP 64-bit block cipher KASUMI (see Chapter 4). The best known attacks on this scheme are given in [371], although these attacks do not seriously threaten the security of the scheme.

The RMAC scheme was proposed in by Jaulmes, Joux and Valette [356]. Its inclusion in a draft standard published by NIST in 2002 [450] attracted a large number of negative comments, and it no longer appears to be a candidate for standardisation. A series of attacks against RMAC have been proposed (see, for example, [370, 372]) which, whilst not invalidating it, raised doubts as to its claimed superiority to other schemes.

The XCBC scheme was originally proposed by Black and Rogaway [64]. Subsequently Kurosawa and Iwata proposed a two-key version TMAC [379], and the same authors then proposed a one-key version OMAC [349]. Whilst these schemes are provably secure, some anomalies in the design of TMAC and OMAC have recently been identified [422].

An attack on ISO/IEC 9797-1 MAC algorithm 5 was described in 2003 by Joux, Poupard and Stern [359]. As a result, MAC algorithms 5 and 6 are likely to be omitted from the next edition of ISO/IEC 9797-1, since they do not appear to offer significant advantages over other standardised CBC-MAC schemes (and they are much less efficient).

A series of tables in Annex B of ISO/IEC 9797-1 provide a detailed guide to the best known attacks on all the standardised CBC-MAC schemes.

In recent years considerable progress has been achieved in developing mathematical proofs of the security of CBC-MAC schemes. Whilst details of these proofs are beyond the scope of this book, we briefly review the main known results. The first main result regarding provably secure CBC-MAC schemes was achieved in 1984 by Bellare, Kilian and Rogaway [48], who showed that SMAC is secure for fixed-length messages. In 2000, Petrank and Rackhoff [466] proved that EMAC is secure if the message length is a multiple of n, and hence is also secure as long as the padding method is 1-1 (i.e. Padding Method 2 or 3 is used). Proofs of security also exist for all the recently proposed schemes, including RMAC [356], XCBC [64, 351], TMAC [351, 379], and OMAC [349, 351]. Whilst ARMAC and MacDES do not possess proofs of security, heuristically one would expect them to be at least as secure as EMAC, since they involve adding one encryption operation to the EMAC construction. A proof of security for 3GPP-MAC was published in 2003 [209], but the proof was shown to be flawed later in the same year [350]; indeed, it was shown that a proof of security for 3GPP-MAC in the 'standard' framework is impossible to achieve. However, by making a slightly stronger, albeit reasonable, assumption about the security of the block cipher, Iwata and Kohno [348] have provided a proof of security for 3GPP-MAC.

§7.4

MDx-MAC was proposed by Preneel and van Oorschot [476] in 1995. HMAC was proposed in 1996 by Bellare, Canetti and Krawczyk [44], as a solution to problems with simpler, flawed hash-based MAC constructions involving simply concatenating a key with the data and then applying a hash-function. Such MAC schemes are susceptible to forgery attacks arising from the extensible property of hash-functions (see Chapter 6). HMAC was first standardised in Internet RFC 2104 [377], before its adoption in ISO/IEC 9797-2 [286]. It has since also been adopted as a US Federal Standard in NIST FIPS PUB 198 [449].

§7.5

MAA was originally proposed in 1984 by Davies [131]. The best known attack on MAA is due to Preneel, Rijmen and van Oorschot [475]. PMAC was proposed in 2001 by Black and Rogaway, who submitted it for consideration by NIST. The scheme was not formally published until 2002 [65].

Chapter 8

Digital signatures

8.1   Definitions and Basic Properties

8.2   Standards for digital signatures

ISO/IEC 9796-3 and all three parts of ISO/IEC 14888 are currently being revised as part of a major reorganisation of ISO/IEC signature standards. This reorganisation will involve all the elliptic curve based signature schemes currently standardised in ISO/IEC 15946 parts 2 and 4 being included in either ISO/IEC 9796-3 or ISO/IEC 14888-3. More specifically, the scopes of the revised standards will be as follows:

- ISO/IEC 9796-3 (2nd edition) will, as at present, be concerned with reversible digital signature schemes based on discrete logarithms. It will include all the mechanisms specified in the current 1st edition of ISO/IEC 9797-6 as well as all the reversible elliptic curve based schemes specified in ISO/IREC 15946-4.

- ISO/IEC 14888-1 (2nd edition) will provide an updated and generalised model for the non-reversible signature schemes specified in parts 2 and 3 of ISO/IEC 14888.

- The 2nd edition of ISO/IEC 14888-2 will be concerned with non-reversible signatures schemes whose security rests on the difficulty of integer factorisation. This revised standard will therefore contain all the factorisation-based mechanisms from the 1st editions of ISO/IEC 14888-2 and ISO/IEC 14888-3, together with certain new mechanisms developed since the 1st editions were published.

- ISO/IEC 14888-3 (2nd edition) will specify non-reversible signature schemes based on discrete logarithms. This new standard will therefore include all the discrete logarithm based mechanisms from the current versions of ISO/IEC 14888-2 and ISO/IEC 14888-3, as well as all the mechanisms from ISO/IEC 15946-2.

The end result of this reorganisation should be two rather more consistently structured series of signature standards.

8.3 The Digital Signature Algorithm (DSA)

8.4 RSA-based signature schemes

8.5 Digital signatures and the law

8.6 Choosing a digital signature scheme

8.7 Notes

§8.1

The idea that a digital signature could replace a handwritten signature was first proposed in the seminal paper by Diffie and Hellman [138]. This was also the paper that first introduced the notion of asymmetric cryptography. Whilst this paper introduced the idea of a digital signature, it wasn't until about a decade later that the security requirements for a digital signature scheme that we now accept as being correct were introduced.

The notion of forgery that we have used in Section 8.1 was first introduced by Goldwasser, Micali and Rivest in a paper published in 1988 [183]. Before this time it was considered impossible to find a signature scheme that was unforgeable in this sense.

The stronger notion of forgery, where an attack is deemed successful if the attacker forges a signature for a new message or finds a new signature for a previously signed message, was introduced later – see, for example, [179].

It is, as was stated in the main body of the text, unclear how useful the stronger notion of forgery is. It is possible to imagine a situation where finding such a forgery would break the intent of the system: consider, for example, a situation where Alice orders drinks from Bob online. Alice may repeatedly send in the same order, and hence the same message, and so Bob might be concerned about making sure that a new message he receives is genuine and not just an old message being re-sent by an attacker. (This property is called message freshness and is quite a common problem in designing security protocols — see Chapter 10). In order to convince himself that a message is genuine, he requires Alice to digitally sign the message and only believes that the message is genuine if it contains a new signature that he has not seen before.

Such a system would require that the signature scheme used satisfied the stronger notion of unforgeability in order to work. Such a system would also be unwieldy and is unlikely to be used in practice, as more elegant solutions to the freshness problem exist (see Chapter 10).

For deterministic schemes, where each message has only one possible signature, the two notions of unforgeability are equivalent.

By now it should not come as much of a surprise for the reader to discover that

descriptions of many popular digital signature schemes can be found in Menezes, van Oorschot and Vanstone [407]. A more mathematical treatment of the field of digital signatures can be found in Stinson [513].

§8.1.2

The example of how to construct a reversible signature scheme from a non-reversible signature scheme demonstrates how it is necessary to send the message along with signature when using a non-reversible scheme. So, in practice, the reversible signature scheme that we constructed is often the scheme that is actually used.

We did not show that it is possible to construct a non-reversible signature scheme from a reversible signature scheme.

If $\mathcal{S}$ and $\mathcal{V}$ are the signing and verification algorithms of a reversible signature scheme then it is possible to construct a non-reversible signature scheme by setting the signing and verification algorithms, $\mathcal{S}'$ and $\mathcal{V}'$, to be

$$\mathcal{S}'(m, s_X) = \mathcal{S}(m, s_X) \tag{8.1}$$

and

$$\mathcal{V}'(m, \sigma, P_X) = \left\{ \begin{array}{ll} valid & \text{if } m = \mathcal{V}(\sigma, P_X) \\ invalid & \text{otherwise} \end{array} \right. \tag{8.2}$$

Unlike the previous example, where a reversible scheme was constructed from a non-reversible scheme, this scheme is of little use and is very unlikely to be used in practice.

§8.1.3

Identity-based cryptography, i.e. asymmetric cryptography where the public key can be derived from the recipient's identity, was first introduced by Shamir [499] and has huge advantages. Because the public key is intrinsically bound to the identity of the entity to whom the key belongs, there is no need to install an expensive public key infrastructure to authenticate that key. Whilst we have not explicitly stated it, it is important to know which "domain" a user belongs to before attempting to derive their public key. This domain will define exactly how to derive the public key from a user's identity.

However there are also some problems that are intrinsically associated with using identity-based cryptography. Since a user's public key is defined by their identity, the key generation algorithm can no longer be a random process but must be deterministic. In order to make this process secure, private keys must be generated by a trusted third party that has some extra, secret knowledge about the signature scheme. This means that the trusted third party has complete control over the key generation process and has access to the private key of all the other entities in the system.

There is also a problem with revocation. Once a private key has been issued for an identity by the trusted third party, that private key will be valid forever. Hence there must be some extra mechanism in place to inform users if a public key is revoked. Online key status discovery protocols, as discussed in Section 13.6 of Chapter 13, are particularly useful in this respect. Another interesting solution is

to derive a public key from a combination of the user's identity and the current date [84]. The user will only be able to obtain the associated private key if the TTP that controls key generation will issue that private key to the user; hence, the TTP can revoke a user simply be refusing to issue it with the correct private keys for a particular date. The key revocation problem will be discussed in more detail, along with certificate-based public-key infrastructures, in Chapter 13.

§8.2

The Digital Signature Algorithm, contained in the Digital Signature Standard [442], is also contained in several other important standards including ANSI X9.30.1 [4], ISO/IEC 14888-3 [267] and IEEE 1363 [221].

A standardised elliptic curve version of the DSA (known as ECDSA) also exists [8, 221, 292, 442]. Elliptic curves are complex mathematical structures that appear to have some useful cryptographic properties. A good introduction to elliptic curve cryptography, including information on the ECDSA, is given by Hankerson, Menezes and Vanstone [202]. More technical information on the use of elliptic curves in cryptography can be found in Blake, Seroussi and Smart [68], and the security of ECDSA is discussed in detail in [69].

The DSA and ECDSA signature schemes have also be recently evaluated by the NESSIE project in terms of their security and performance [456, 457]. They were evaluated against several other signature schemes, some of which have also been standardised, and judged to be amongst the best of the proposed schemes.

The other signature scheme endorsed by the financial sector is known as rDSA and is specified in ANSI X9.31 [7].

The signature scheme contained in ISO/IEC 9796 [233], the first general purpose ISO/IEC standard for signatures, was attacked by Coron, Naccache and Stern [123] although they do not manage to completely break the scheme. The scheme was eventually broken by Coppersmith, Halevi and Jutla [119] and by Grieu [195]. As a result of these attacks, ISO/IEC 9796 was withdrawn. There are no known attacks against the schemes contained in either ISO/IEC 9796-2 [295] or ISO/IEC 9796-3 [285]. The 2nd edition of ISO/IEC 9796-3 (which has been expanded to incorporate the elliptic curve based mechanisms specified in ISO/IEC 15946-4 [305]) is currently at the committee draft stage [310].

The general purpose ISO/IEC standard on non-reversible signature schemes is ISO/IEC 14888. It consists of three parts: a general introduction [266], a series of identity-based mechanisms [272] and a series of certificate-based mechanisms [267]. Many of the schemes contained in ISO/IEC 14888-3 can also be implemented using elliptic curve techniques. These schemes are standardised in ISO/IEC 15946 part 2 [291]. The revised and re-organised parts 2 and 3 of ISO/IEC 14888 are currently at working draft stage [319, 320]. The new text for ISO/IEC 14888-3 incorporates all the mechanisms currently specified in ISO/IEC 15946-2 [291].

As we have mentioned, IETF RFCs have tended to endorse other signature standards, such as the Digital Signature Algorithm, rather than standardise new signature schemes of their own. IETF documents and standards, such as IETF RFC 3075 [147], tend to concentrate on describing the practical uses of signature schemes.

§8.3

The Digital Signature Algorithm was first introduced by Kravitz as a proposed NIST FIPS standard in 1991 and was officially declared a standard in 1994 [442]. It is also the subject of a U.S. patent (U.S. patent number 5,231,668) although no licence is required for its use.

For a proof of the correctness of the DSA algorithm see Stinson [513]. A short proof is also contained in an appendix of NIST FIPS 186-2 [442].

It should be noted that there is a small chance that the DSA algorithm will fail to verify a valid signature. This happens if $S \equiv 0 \bmod q$. In this case it is impossible to invert S modulo q, i.e. there is no integer value W such that $S \cdot W \equiv 1 \bmod q$. Hence the verification algorithm fails at step 1.

Also, if the DSA is to be used by more than one entity in a system, it is not necessary for each entity to generate a complete new public key. The public parameters of the system (p, q and g) can be used by every participant. This means that each entity only has to generate a secret key x between 1 and $q-1$, and a public value $y = g^x \bmod p$.

It is easy to show that the DSA signature scheme is insecure whenever the same value k is used to sign two different messages. Suppose (R, S) and (R, S') are signatures for two different messages m and m', but that both of these signatures have been computed using the same value of k. It is easy to see that

$$S - S' = k^{-1}(\mathrm{hash}(m) - \mathrm{hash}(m')) \bmod q \tag{8.3}$$

and so

$$k = \frac{\mathrm{hash}(m) - \mathrm{hash}(m')}{S - S'} \bmod q \,. \tag{8.4}$$

From here it is easy to recover the private key x as

$$x = \frac{Sk - \mathrm{hash}(m)}{R} \,. \tag{8.5}$$

It should be clear that this attack can also be used if an attacker can find out the value k used to create a signature (R, S) for a message m. Nguyen and Shparlinski [458] have gone further and shown that it is possible to recover the private key if only a fraction of the bits of k are known to the attacker. Bleichenbacher [74] also proposed an attack against DSA by noting that, in the original specification of the algorithm, small values of $k \bmod q$ were more likely to occur than larger ones. The DSS was subsequently changed to make sure that k is chosen randomly from all possible values.

§8.4

The use of RSA as a signature scheme was first proposed in the initial paper on the RSA scheme by Rivest, Shamir and Adleman [484]. The method they proposed is very similar to the methods used today — to prove the integrity of a message by supplying an encrypted version of that message or a hash-code of that message. Since that paper the main efforts in this area have been to try and find efficient ways of securely formatting the message representative before encryption.

More details on the improved RSA signing function can be found in ISO/IEC 9796-2 [295].

It is possible to adapt the given scheme to provide partial message recovery. It should be noted that the current scheme can only sign messages that are at most the size of the modulus less the size of the *hash*, *header* and *trailer* fields. The scheme can be extended to sign messages of any length. Here we split a message m into two parts: a recoverable part m_1 and a non-recoverable part m_2. The recoverable part of the message m_1 must be short enough that it can be included in the message representative. The message representative is constructed as before but only the recoverable part of the message is included, i.e. the message representative has the form:

$$\alpha = header||padding||m_1||hash||trailer\,. \tag{8.6}$$

It is important that the hash-code is still computed by applying the hash function to the whole message m.

Signature verification is given in the obvious way. The verification algorithm recomputes the message representative from the signature and checks that the hash-code is valid using both the recoverable part of the message contained in the message representative and the non-recoverable part which must be sent along with the signature. If the signature is valid (i.e. the hash-codes match) then the recoverable part of the signature is released.

Unlike the DSA scheme, RSA-based signature parameters cannot be used by more than one user. If two users wish to use RSA based signature schemes then they must both compute completely separate public and private keys, and no parameters can be shared or the entire scheme is compromised.

§8.5

There are several technical (i.e. non-legal) books that discuss the status of digital signatures in law, including Adams and Lloyd [25] and Ford and Baum [171]. Rosenoer [491] is, by now, a little out of date but does contain material on earlier developments, such as the Utah Digital Signature Act. The definitions of "contract" and "signature" in Section 8.5 are adapted from this latter source.

Electronic signatures are given legal status in the United States by the ESIGN Act [193]. This follows on from certain state-wide legislation such as the Utah Digital Signature Act [516] and the advice of the American Bar Association [31].

It is interesting to note that there are some unusual definitions and seemingly paradoxical results of the US legislation. For example, the ESIGN Act specifically notes that a recording of an oral communication shall not qualify as an electronic record but that a recorded sound may act as an electronic signature. It is also interesting to note that the Utah Digital Signature Act defines an "asymmetric cryptosystem" as "an algorithm or series of algorithms which provide a secure key pair." This somewhat contradicts the definitions we have been using in this book!

EU Directive 1999/93/EC [152] mandates that all European Union member states should enact legislation that allows electronic signatures to be presented as evidence in court. It also notes that the EU has the right to recommend digital signature schemes by publishing references to well-defined standards. Such a recommendation

has been published as ETSI SR 002176 [163] and includes references to ISO/IEC 14888-3 [267], IEEE 1363 [221] and FIPS 186-2 [442].

The UK has enacted this EU directive in the Electronic Communications Act [191]. Advice on interpreting this Act can be found in the explanatory notes provided by the UK government [192] and the Law Commission report [386].

Both the US and the EU legislation recognise the need for a digital signature to be verified using a public key that has been correctly validated (see Chapter 13), and both the ESIGN Act and the EU Directive 1999/93/EC states the requirements that a certification authority (CA) must satisfy in order to be considered secure. The IETF have produced a profile for qualified certificates (the EU notion of a secure certificate) for use on the Internet. This profile is contained in IETF RFC 3039 [494].

Chapter 9

Non-repudiation mechanisms

9.1 Introduction

9.2 Standards for non-repudiation

9.3 Non-repudiation model and services

9.4 Non-repudiation using symmetric cryptography

9.5 Non-repudiation using asymmetric cryptography

9.6 Time-stamping and non-repudiation

9.7 Notes

§9.1

Zhou's book on non-repudiation [530] provides a very detailed analysis of the topic. Earlier work of note on the topic includes the 1997 Ph.D. theses of Roe [485] and Zhou [529]. A discussion of the concept of repudiation in law can be found in Appendix I of [171].

§9.2

ISO/IEC 13888 Parts 1–3 were published in 1997 and 1998 [258, 259, 265]. Part 1 was recently revised, and the 2nd edition was published in 2004 [304]; however, it only contains minor differences to the first edition.

§9.3

A detailed discussion of non-repudiation services, and mechanisms for the provision of such services, can be found in chapter 9 of [171].

§9.4

A number of authors have proposed more complex non-repudiation protocols designed to force message recipients to provide the evidence necessary to provide non-repudiation of delivery. For example, Zhou and Gollmann [532] proposed use of a TTP which does not release the key necessary to decrypt a message until it receives a signed receipt (essentially an NRD token); to prevent denial of service attacks where messages from the TTP are blocked, the TTP is required to post the

decryption key for the message on a public web site. This and other solutions are also discussed in [531] (see also [530]).

§9.5

The use of digital signatures to provide non-repudiation services is in most cases inextricably linked with the use of Public Key Infrastructures (discussed in Chapter 13) and TTP services, especially time-stamping services (discussed in Chapter 14).

Chapter 10

Authentication protocols

10.1   Introduction

10.2   Standards for entity authentication protocols

10.3   Cryptographic mechanisms

10.4   Timeliness checking mechanisms

10.5   Authentication using symmetric cryptography

10.6   Authentication using asymmetric cryptography

Table 10.4 was based on the FCD text of ISO/IEC 9798-5. As a result of changes made in the FDIS text, the mechanism in ISO/IEC 9798-5 clause 8 exists only in two variants (and not three), known as GPS1 and GPS2; as a result the text '(GPS1/2/3)' should read '(GPS1/GPS2)'.

10.7   Manual authentication protocols

10.8   Choosing an authentication protocol

10.9   Notes

§10.1

Chapter 10 of Menezes, van Oorschot and Vanstone [407] provides a more detailed discussion of authentication protocols. A more recent comprehensive discussion of authentication protocols can be found in Boyd and Mathuria's book [88].

The first discussion of authentication protocols is contained in the landmark 1979 paper of Needham and Schroeder [454]. This paper contains a series of protocols based on different cryptographic primitives, and has set the context for the now large literature on authentication protocols.

§10.2

The first published standard for authentication protocols was the 1988 edition of X.509 [117]. One section of this CCITT Recommendation contains a series of three authentication protocols based on the use of digital signatures (under the heading

of 'strong authentication'). Unfortunately, one of the three protocols contained a flaw, as discovered by Burrows, Abadi and Needham [100, 101, 102, 103] (see also [218]). This flaw was rectified in the second and subsequent editions of the recommendation [324, 335, 336] (see also the parallel ISO/IEC standard, ISO/IEC 9594-8 [289]).

ISO work on standards for authentication protocols started in the late 1980s, culminating in the publication in the early-mid 1990s of the first editions of Parts 1-3 of ISO/IEC 9798 [234, 243, 244]. Work on Part 4 commenced as the first three parts neared completion, with the first edition appearing in 1995 [246]. All of these four parts were then revised, essentially for editorial reasons (no changes were made to the mechanisms), and the revised standards appeared in the late 1990s, [260, 277, 269, 278]. The original motivation for ISO/IEC 9798 Parts 2 and 3 was provided by Needham and Schroeder [454].

Work on ISO/IEC 9798-5 started somewhat later, and the standard was finally published in 1999 [279]. A revised version, containing a larger selection of mechanisms, is now nearing publication [318]. ISO/IEC 9798-6 [315], currently at FCD stage, is of much more recent origin, work only starting in early 2003. The standard adopts techniques previously proposed for Bluetooth, and designed to enable mobile devices owned by a single individual to set up secure links.

NIST FIPS Pub. 196 [440] is based on ISO/IEC 9798-3 and was published in 1997.

The Kerberos protocol [512, 455] was developed as part of the Athena project at MIT, quite independently from the ISO/IEC work. The Kerberos protocol has evolved over time, so that the version specified in RFC 1510 [374] is actually Version 5 of the scheme. The S/KEY protocol (specified in RFC 1760 [200]) is closely based on an original idea of Lamport published in 1981 [382]. RFC 1704 [201], dating back to 1994, gives a lot of useful general advice on authentication methods for use across the Internet. The *Distributed Authentication Security Service* DASS protocol is specified in RFC 1507 [368].

§10.3

Using a combination of symmetric encryption and an MDC to provide origin authentication and integrity protection for a message is not a recommended approach. Both the method for encryption and the MDC technique need to be selected with considerable care. Some versions of Kerberos possess vulnerabilities arising from the use of an inappropriate MDC (see [54]). For a more detailed discussion of these issues see Section 9.6.5 of [407].

There is a large literature on zero knowledge protocols; Section 10.4 of [407] contains a useful overview.

§10.4

The classic 1978 paper of Lamport [381] provides a detailed discussion of the use of various types of time-stamps in a general distributed systems setting. The need to keep a log of recently received messages to prevent replays of messages within the 'window' of time-stamp checking was first discussed by Lam [380].

There are a number of other possible issues with the use of time-stamps. Gong [188] has pointed out that if an authentication protocol is executed when one party has

an incorrectly synchronised clock, the messages sent in that protocol may be used later to impersonate one of the entities even after all clocks have been correctly synchronised. Bellovin and Merritt [53, 54] also provide a discussion of the risks of using time-stamps.

One important scheme for providing securely synchronised clocks is the Network Time Protocol (NTP), Version 3 of which is specified in RFC 1305 [417]. An simplified version of NTP for Internet use, known as the Simple Network Time Protocol (SNTP) is specified in RFC 2030 [418]. The NTP protocol uses symmetric cryptographic techniques, and ongoing work within the IETF Secure Time Working Group is aimed at specifying how public key cryptography can be used to support NTP [419].

The possibility of preplay attacks on protocols using predictable nonces was first pointed out by Gong [189].

§10.5

The existence of reflection attacks, the motive for including the identifier for the recipient within the scope of encryption and MAC computations in symmetric cryptography based protocols, was first pointed out in [420]. An alternative to the use of identifiers (also pointed out in ISO/IEC 9798-2 and 9798-4) is to employ unidirectional keys, i.e. separate keys for protecting messages sent from A to B and from B to A.

The limitations of S/KEY in the case where the host can be impersonated, appear to have been observed by a number of authors in the mid-1990s — see, for example, [425] or Note 10.7 of [407].

AKEP2 was first proposed by Bellare and Rogaway in 1993 [51], and is given as Protocol 12.20 in [407]. A version of this protocol is included in a 1999 Internet draft [144], although this draft has now expired.

Note that neither of the TTP protocols standardised in ISO/IEC 9798-2 are quite the same as the Needham-Schroeder protocol because of the need to address the problem identified by Denning and Sacco [135].

If Kerberos is used with a guessable password as the long-term secret shared by the client and the authentication server, then password guessing attacks may be possible. This and other possible security issues with Kerberos are discussed by Bellovin and Merritt in [53, 54], who also propose possible solutions to the password guessing problem. For details of the current version of Kerberos see

```
http://web.mit.edu/kerberos/www.
```

§10.6

The ID-based unilateral authentication protocol specified in clause 5 of ISO/IEC 9798-5 is a generalisation of the Fiat-Shamir protocol [168] due to Guillou and Quisquater [196]. The integer-factorisation based unilateral authentication protocol given in clause 6 of ISO/IEC 9798-5 is the QG2 protocol of Guillou and Quisquater [197]. The unilateral authentication protocol based on discrete logarithms in ISO/IEC 9798-5 clause 7 is due to Schnorr [497]. The GPS1 and GPS2

unilateral authentication mechanisms, specified in clause 8 of the draft 2nd edition of ISO/IEC 9798-5, are due to Girault, Paillès, Poupard and Stern [176, 177, 472]. Finally, the unilateral authentication protocol based on asymmetric encryption given in clause 9.3 of ISO/IEC 9798-5 is due to Brandt et al. [91].

Early versions of the ISO/IEC 9798-3 three-pass mutual authentication protocol using signatures and nonces were subject to interleaving attacks; see, for example, [186].

The mutual authentication mechanism based on asymmetric encryption is known as the Helsinki protocol. An earlier version of this protocol was shown to be flawed by Horng and Hsu [210], and subsequently fixed in [429]. Interestingly, the flaw and the fix mirror the changes proposed after similar problems were identified in a Needham and Schroeder protocol by Lowe [393, 394]. If the asymmetric encryption function in use has the non-malleability property (see, for example, [47]), then the hash-codes do not need to be included in messages M_1 and M_2 of the Helsinki protocol.

§10.7

The problem of initialising personal devices is discussed by Stajano and Anderson in [506, 507]. For a general guide to manual authentication see [172, 174]. The current version of ISO/IEC 9798-6 (the first CD [299]) contains a total of four different manual authentication mechanisms. Two of these mechanisms derive from work of Gehrmann and Nyberg [173]. The other two mechanisms are due to Larsson [384] and Jakobsson, [353].

Some of the ISO/IEC 9798-6 schemes may also be included in a future version of the Bluetooth standards. The existing Bluetooth specifications already contain a solution to device imprinting, but this solution has well-known security shortcomings if the initial exchange between devices can be wiretapped [174, 355].

The first protocol of this type was proposed by Maher, [396], who proposed using manual techniques to authenticate a standard Diffie-Hellman key establishment process (see Chapter 12). However, the techniques contained in ISO/IEC 9798-6 reduce the work involved for the human operator of the devices.

§10.8

The Bellare and Rogaway AKEP2 protocol possesses a proof of security [51]. Blake-Wilson, Johnson and Menezes [70, 71] examined signature-based authentication protocols, and have, amongst other things, shown that the the three-pass signature-based protocol from ISO/IEC 9798-3 is secure.

For further details about proofs of security for authentication protocols the reader is referred to the books of Ryan et al. [493] and Boyd and Mathuria [88].

Chapter 11

Key management frameworks

11.1   Standards for Key Management

11.2   Definitions and Basic Properties

11.3   The General Framework

11.4   The ANSI X9.24 Framework

11.5   Notes

This chapter covered the key management frameworks of three separate bodies.

The general details were taken from ISO/IEC 11770-1 [254]. The remaining two parts [255, 271] of this standard will be dealt with in the next chapter. This part of the standard is almost unique in that it concentrates solely on the key management framework and provides no details of mechanisms that might be used to implement this framework.

The approach of ANSI X9.24 [30] and ANSI X9.17 [3], now withdrawn [10], is very different. These standards approach the subject in terms of rules and requirements that must be satisfied. These rules and requirements imply a key management framework but do not explicitly give one. To a certain extent this means that the framework is open to interpretation by the developer but, in reality, the requirements are so strict that it would be difficult to misinterpret them.

The withdrawal of ANSI X9.17 has left something of a void in the ANSI standards portfolio. The document that officially withdrew the standard, ANSI X9 TG26 [10], is more than a simple statement: it details an entire strategy describing how the techniques of ANSI X9.17 could be replaced with newer techniques with minimum risk. However, whilst it cites newer ANSI standards as replacements for the key establishment mechanisms contained in ANSI X9.17, it does not appear to specify a new framework for wholesale key management within the financial sector. It is unclear whether the revised version of ANSI X9.24 is meant to fill this role, or whether ANSI X9.17 has been superseded by the the corresponding ISO standard, ISO 8732 [226].

Soon after the ANSI X9 standards were originally published, the ISO technical committee on banking (ISO TC68) began work on producing corresponding international standards. The results were ISO 8732 [226], which is based on ANSI X9.17, and ISO 11568 [238, 239, 240, 263, 264, 270], which is based on ANSI X9.24. Of particular relevance to this chapter is ISO 11568-1 [238], which introduces the concept of key management, ISO 11568-2 [239], which introduces many of the general ideas contained in Section 11.2, and ISO 11568-3 [240], which specifies the key life cycle for secret (symmetric) keys. The framework that these documents establish is almost identical to that of ANSI X9.24.

Of the remaining parts of ISO 11568, parts 4 and 5 [263, 264] discuss the public key life cycle and will be discussed in chapter 13. The last part, ISO 11568-6 [270], contains descriptions of key management schemes that are approved for use in retail

situations. As this does little to enlighten the reader as to the technical reasons for implementing a key management scheme in a particular way it will not be discussed further.

There are several good introductory texts available on key management. Chapter 12 of Menezes *et al.* [407] serves as a good, if somewhat technical, introduction. Other good sources include Kou [376] and Davies and Price [133].

Chapter 12

Key establishment mechanisms

12.1   Definitions and Basic Properties

12.2   Standards for Key Establishment

Part 4 of ISO/IEC 11770, currently under development, covers key establishment mechanisms based on weak secrets (i.e. human-memorable secrets such as passwords). These mechanisms, discussed in more detail in Section 12.6, are typically based on asymmetric cryptography, although they are rather different in nature from the mechanisms discussed in Section 12.5.

12.3   Physical Mechanisms

12.4   Mechanisms using symmetric cryptography

Recently, several attacks has been found against Key Establishment Mechanism 12 from ISO/IEC 11770-2. One attack uses a method similar to the attack noted by Boyd on the ISO 8732 key establishment protocol discussed in Section 12.4.2, and allows an attacker to force a user to re-use an expired key. A second attack uses the possibility of a poor implementation to deceive a user into believing he is executing the protocol with another registered user, when in fact he is interacting with the attacker.

12.5   Mechanisms using asymmetric cryptography

Asymmetric key agreement mechanisms typically provide both parties with a shared secret value from some set of possible outputs. The set of possible outputs is usually related to some mathematical function (for example, the set of integers modulo a prime number p). In order to derive a shared symmetric key, both parties input this shared value to an agreed hash function. This process, as has been noted before, is known *key extraction.*

However, sometimes the users wish to share a key that is longer than the output of the hash function they have agreed to use. Several standards, including ANSI X9.42, ANSI X9.63, and IEEE P1363a, standardise a mechanism to produce these long key values. This involves concatenating the hash codes produced by applying the hash function to both the shared secret value and an increasing counter value. Recently, doubt has been cast on this technique by Adams, Krammer, Mister and Zuccherato, who have shown that the keys produced by this technique do not occur with equal probability. However, their objections, whilst valid, do not seem to constitute a practical attack against the key establishment mechanisms.

12.6 Key establishment based on weak secrets

12.7 Key establishment for mobile networks

12.8 Choosing a key establishment scheme

12.9 Notes

§12.1

Owing to the peculiar evolution of key management systems — an evolution based on best practices in industry rather than by academic research — it is difficult to track down the origin of many of the important concepts in key management. Crucial concepts such as key authentication, key confirmation and key control have grown up from the use of keys rather than from academic discussion, and the development of key management standards by informed professionals has played an important role in the evolution of these ideas.

This chapter only introduces some of the many possible mechanisms that can be used to established shared secret keys. For more information on this subject the reader is referred to Boyd and Mathuria [88]. The basic principles of key establishment using symmetric and asymmetric techniques are also discussed in Stallings [508]. There is also a nice summary of the ISO 8732 standard for key establishment in the wholesale banking sector in Davies and Price [133].

It should be noted that, whilst standard key agreement protocols are less suited to generating the complex keys required by asymmetric applications, key agreement protocols can still be used to generate these keys. A key agreement protocol will typically ensure that both parties can establish a suitably random binary string of some pre-determined length in a confidential manner. If this random string is used as the random bits that a key generation algorithm (see Chapters 4 and 8) requires, then both parties can generate the same asymmetric keys by running the same key generation algorithm.

§12.2.1

Four main standard bodies have produced standards for key establishment using symmetric techniques. Two of these are applicable only to specific sectors: the ISO 8732 standard [226], which is applicable to the financial sector, and the 3GPP TS 33.102 standard [160], which is only applicable to the mobile phone sector.

A general key establishment standard has been produced by the ISO/IEC JTC1 committee, of which ISO/IEC 11770-2 [255] deals with key establishment using symmetric techniques.

The Kerberos protocol is specified in IETF RFC 1510 [374]. Other IETF protocols include the Photuris session-key management protocol, which is contained in IETF RFC 2522 [366].

§12.2.2

There are two main approaches to key establishment using asymmetric techniques. The general ISO/IEC JTC1 standard, ISO/IEC 11770-3 [271], defines several key establishment mechanisms based on a general function that satisfies certain security properties. Hence the standard does not, strictly speaking, define any complete protocols. However there is a tacit understanding that these protocols should be instantiated using the Diffie-Hellman function (see Section 12.5.1).

Other standards are more specific. Almost all the standardised key agreement protocols are based on the Diffie-Hellman protocol, and this is standardised in ANSI X9.42 [12], IETF RFC 2631 [481], IEEE 1363 [221, 223], and RSA PKCS #3 (see Chapter 4 for more information about the RSA PKCS series of standards). There are also several standardised elliptic curve versions of the Diffie-Hellman protocol, see ISO/IEC 15946 [292], ANSI X9.63 [13] and IEEE 1363 [221, 223].

The second class of techniques, namely asymmetric key transport techniques, are usually based on asymmetric encryption and digital signature schemes. Asymmetric key transport schemes are standardised in ISO/IEC 11770-3 [271] and ISO 11166 [236, 237].

The IETF schemes are standardised in RFC 2246 [137] (the TLS protocol), RFC 2409 [203] (the IKE protocol) and RFC 2412 [463] (the OAKLEY protocol). These are fairly high level descriptions concerned more with the describing the messages that need to be passed between two computers to facilitate establishing a key, rather than concentrating on the key establishment technique itself. An extension of the TLS protocol that uses the Kerberos authentication/key establishment protocol is described in RFC 2712 [406].

§12.3

The most common situation in which keys are distributed physically is in the distribution of PINs for ATM cards. Here the "key" is distributed using several sealed packages: the outer letter which contains the address of the recipient and the sealed inner letter which contains the actual PIN.

The idea of key splitting can be extended so that the key is split between more than two parties. The simplest way to split a key K between n users is to generate n key fragments $k_1, \ldots k_n$ such that

$$K = k_1 \oplus k_2 \oplus \ldots \oplus k_n. \tag{12.1}$$

This has the disadvantage that the key cannot be legitimately recovered unless all the key fragments are correctly received. More complex schemes exist in which the key is split between n users but the key can be recovered provided that some smaller (threshold) number of key fragments are correctly received. These schemes are known as *secret sharing schemes*, the first examples of which were independently given by Blakley [72] and Shamir [498] in the late 1970s.

§12.4

The ISO/IEC 11770-2 key establishment mechanisms that use direct communication are strongly based on the ISO/IEC 9798-2 entity authentication schemes [277] (see Chapter 10).

The idea of using a trusted third party to facilitate key establishment was first introduced by Needham and Schroeder [454] in 1978. Whilst one of their protocols was subsequently broken [43, 135], the idea remained.

All of the ISO/IEC 11770-2 key establishment mechanisms that make use of a key distribution centre are based on the Bauer, Berson and Feiertag correction [43] to the Needham and Schroeder protocol. The ISO 8732 protocol, described in Section 12.4.2, is similar to the key establishment protocol proposed by Boyd [86] (although the Boyd protocol uses nonces for freshness instead of timestamps, and was published about a decade after the ISO 8732 protocol was released). The Kerberos key distribution protocol [455, 512] is discussed in detail in Chapter 10.

The attack against the ISO 8732 protocol described in Section 12.4.2 was noted by Boyd [87].

The attack against Key Establishment Mechanism 12 of ISO/IEC 11770-2 was presented by Cheng and Comley [110].

§12.5

The Diffie-Hellman protocol was introduced in the famous paper by Diffie and Hellman [138]. This paper introduced both the Diffie-Hellman "special function" described in Section 12.5.1 and the Diffie-Hellman key agreement protocol described in Section 12.5.2. The tweaked version of the Diffie-Hellman function, in which small subgroups are avoided, has been attributed by Boyd and Mathuria [88] to Vanstone but no original paper seems to exist on the subject.

The problems with extracting long keys were noted by Adams, Krammer, Mister and Zuccherato [23]. This technique is also used in the ISO/IEC 18033-2 standard on encryption; however, the problems noted by Adams *et al.* do not appear to pose a practical threat here either.

It should be noted that special function P defined in Section 12.5.1 is denoted by F in ISO/IEC 11770-3. We have changed this designation to avoid confusing this function with the keying material.

The more complicated key agreement protocol using nonces, discussed in Section 12.5.2, is actually the MTI A(0) protocol developed by Matsumoto, Takashima and Imai [401]. There have been several proposed attacks against this scheme that suggest it can be broken if it is not implemented carefully – see, for example, [98]. One of the more interesting attacks [360] demonstrates that an attacker can successfully impersonate an entity X (and retrieve the agreed key) when communicating with that entity, i.e. the attacker can impersonate X to X. Obviously, such an attack will not be relevant in most well implemented systems.

The idea that an entity can exert some measure of key control in key agreement protocols by selecting a more favourable key from a selection it has generated using several different parameter sets (for example, when B chooses a nonce that gives a more favourable key in the nonce-based protocol of Section 12.5.2) was first introduced by Mitchell, Ward and Wilson [428].

The station-to-station protocol was first proposed by Diffie, van Oorschot and Wiener [141] in a slightly different format to the protocol discussed here. The original version did not sign A or B's identifiers but symmetrically encrypted the

digital signatures under the newly established key K in order to demonstrate that both entities knew the key K. The adapted version of the protocol we use is discussed in Boyd and Mathuria [88] and has been proven secure by Bellare, Canetti and Krawczyk [45, 105].

The Menezes-Qu-Vanstone (MQV) key agreement protocol [385] is not included in the ISO/IEC standard [271] but does appear in the IEEE 1363 [221], ANSI X9.42 [12] and ANSI X9.63 [13] standards. It uses the fact that when P is the Diffie-Hellman function, i.e. $P(h, g) = g^h \bmod p$, we have certain multiplicative identities:

$$
\begin{aligned}
P(h_1 + h_2, g) &= P(h_1, g) \cdot P(h_2, g) \,, & (12.2) \\
P(h_1 h_2, g) &= P(h_1, P(h_2, g)) \,, & (12.3)
\end{aligned}
$$

and

$$
P(h, g_1 g_2) = P(h, g_1) \cdot P(h, g_2) \,. \qquad (12.4)
$$

For more details, see [385].

The key transport mechanism given in Section 12.5.3 is both efficient and secure, although some concerns have been raised about the fact that the signature is only computed on publicly available information. Hence it is possible for a malicious attacker to substitute the correct signature with his own, and thus attempt to fool B into thinking that the message was from him. This attack only works if the attacker can also change the identifier i_A that has also been encrypted, and even then the attacker still does not learn the value of the key.

§12.6

We have only briefly mentioned the mechanisms and the problems associated with key establishment using weak secrets (passwords). A more comprehensive study can be found in Boyd and Mathuria [88]. The ISO/IEC standard on such mechanisms, ISO/IEC 11770-4, is currently at the CD stage [308].

§12.7

An overview of the key establishment mechanisms used in 3GPP mobile networks can be found in Temple and Regnault [515]. As we have mentioned, the 3GPP key establishment algorithm is very similar to that found in the 2nd generation GSM mobile networks. A good description of this earlier scheme can be found in Hillebrand [207]. Future trends in security for mobile networks are discussed in Mitchell [424].

The 3GPP key establishment scheme described in this section is standardised in 3GPP TS 33.102 [160]. The MILENAGE algorithm set, the example algorithms that 3GPP have provided for the $f1 - f5$ functions, are given in a series of five standards: the general introduction [156], the algorithm specification [161], the implementors' test data [157], the conformance test data [158] and the summary and results of the design and evaluation process [159].

Chapter 13

Public Key Infrastructures

13.1 What is a PKI?

13.2 PKI standards

Two parts of the multi-part retail banking key management standard, ISO 11568, relate to PKI. ISO 11568-4 contains two annexes of particular relevance. Annex B defines rules and requirements for certificate management, as well as specifying mandatory and recommended data elements for inclusion in public key certificates; Annex C provides a similar set of definitions and requirements for attribute certificates. ISO 11568-5 defines a key life cycle for public key cryptosystems; this life cycle has a close relationship to the key life cycle defined in ISO/IEC 11770-1 (see Chapter 11).

13.3 Certificate formats

13.4 Certificate management

13.5 Certificate storage and retrieval

13.6 Certificate status discovery

13.7 Certificate Policies and Certification Practice Statements

13.8 Notes

Because of the potential practical importance of PKIs, there are a number of books on this topic, including those of Adams and Lloyd [24], Austin and Huaman [40], and Feghhi, Feghhi and Williams [166]. Ford and Baum's book on secure e-commerce also provides extensive coverage of PKI issues [171]; indeed, this latter book provides a particularly accessible introduction to the subject.

§13.1

The Handbook of Applied Cryptography [407, page 587] attributes the concept of public key certificate to the 1978 thesis of Kohnfelder [375]. The idea is implicit in the Rivest-Shamir-Adleman paper of February 1978 [484], where the notion of a *public file* signing a message containing an end-user public key is described, and where every user is equipped with the public key for this public file. This public file is playing the role of the CA.

The term PKI is of much more recent origin — it does not even appear in the 1997 Handbook of Applied Cryptography [407]. The earliest published reference to the term appears to be April 1994, when Berkovits et al. published a study on the subject, [55]. Later the same year, Chokhani discussed a US national PKI, [112]. In September 1995 NIST ran an invitational workshop on the subject [439]. The IETF PKIX Working Group was also established in the fall of 1995, with the goal of developing Internet standards needed to support an X.509-based PKI. By the late 1990s the term was ubiquitous.

§13.2

The first work on developing PKI standards predates the term PKI by some years. What has become known as the X.509 certificate format was first standardised in 1988 [117], as part of the first edition of the ITU-T X.500 directory services recommendations (note that they were then referred to as CCITT recommendations). For a general guide to X.500 directories see [107].

Three subsequent editions of this ITU-T recommendation have been published, [324, 335, 336], with the most recent edition (the fourth edition) having been published in 2000. In each case, an aligned ISO/IEC standard, ISO/IEC 9594-8 was published a year or two later, the most recent (third and fourth editions) having been published in 1998 and 2001, [268, 289].

The original work on X.509 was performed as part of the development of the X.500 directory series recommendations. The main initial 'customer' for the standardised public key certificates was the parallel X.400 series of recommendations specifying the operation of an email system. The 1988 version of the X.400 standards incorporated a large range of security features, the key management for which was based on the use of X.509 certificates. Interestingly, while the X.400 recommendations have hardly set the world alight, the X.509 public key certificate format dominates the field.

After the publication of the first edition of the X.509 recommendation, the next main customer for the X.509 certificate format was again a secure email system — this time the Internet Privacy Enhanced Mail (PEM) system, [369]. This scheme again used X.509 certificates as the basis of its key management; however, a number of additional certificate features were required by PEM which were incorporated into the X.509 version 2 certificate format [324]. Subsequent growing interest in deploying X.509 PKIs revealed the need for further additional data elements in a certificate, and these were incorporated into the version 3 certificate format [268, 335].

The PKIX Roadmap is currently only an Internet draft; at the time of writing the latest version was published in January 2003 [39].

ISO/IEC 15945 [290] was published in 2002; the identically worded ITU-T recommendation, X.843, was published a little earlier [339]. ISO/IEC 15945 is concerned with the TTP services (primarily CA services) necessary to support the use of digital signatures. It is to a large extent based on the mechanisms specified in RFCs 2510 and 2511, [22, 433].

The two-part standard ISO 15782 significantly extends the generic PKI standards within a banking context. Part 1 [298] provides a general model and rules for cer-

tificate management. It has a significant degree of commonality with the earlier US banking standard ANSI X9.57 [6]. Part 2 [287] defines banking specific extensions to X.509 certificates, and this too builds upon an earlier US standard, namely ANSI X9.55 [5]. ISO 11568 parts 4 and 5 [263, 264] provide PKI management principles for application in a retail banking environment.

ANSI X9.79-1 [14] provides banking-specific guidance on Certificate Policies and Certification Practice Statements.

A useful general discussion of PKI standardisation, and the need for additional PKI standards, has been provided by Palmer [464].

§13.3

ASN.1 is specified in a series of ITU-T recommendations, X.680-X.683 [341, 342, 343, 344]. ASN.1 encoding rules are given in X.690 and X.691, [345, 346]. A comprehensive guide to ASN.1 can be found in [383], and a helpful brief introduction is given in Appendix C of [171].

The formats for DNS names, IP addresses and URIs are specified in RFCs 1035 [430], 791 [220], and 1630 [56] respectively.

The first version of the PKIX X.509 profile, RFC 2459 [212], was published in 1999; in April 2002 this was superseded by RFC 3280 [215]. Two other PKIX certificate profile documents, RFCs 3279 and 3281 [471, 165] were published at the same time, RFC 3279 superseding RFC 2528 [214].

A second, more specialised, PKIX certificate profile, RFC 3039 [494], covering Qualified Certificates, was published in 2001. RFC 3039 is based on the now superseded PKIX certificate profile, RFC 2459. A useful introduction to qualified certificates is provided in Chapter 6 of [171].

For further details of the X.509-WAPcert and other wireless PKI issues see [129].

The EMV certificate format is defined in Book 2 of the EMV 2000 specifications [150].

§13.4

The Certificate Management Protocol is specified in RFC 2510 [22], and uses the Certificate Request Message specified in RFC 2511 [433]. Both CRM and CMP are also specified in ISO/IEC 15945 [290] and the identical ITU-T recommendation X.843 [339].

A proof of possession technique appropriate for Diffie-Hellman key pairs is defined in RFC 2875 [473]. A survey of proof of possession techniques is provided in [426].

PKCS #7 and PKCS #10, whilst originally produced by RSA Inc., have since been published as Internet RFCs; the latest versions are available as RFC 2315 [364] (PKCS #7 v1.5) and RFC 2986 [460] (PKCS #10 v1.7) — v1.5 of PKCS #10 was previously published as RFC 2314 [363]. The CMC protocol, which builds upon PKCS #10, is specified in RFC 2797 [435]. CMC uses the Cryptographic Message Syntax (essentially a superset of PKCS #7) which is specified in RFC 2630 [211].

§13.5

A more detailed comparison of LDAP version 2 and X.500 directories has been given by Hassler [204].

The PKIX certificate access protocol is defined in RFCs 2559 and 2587 [78, 79]. This is based on the IETF LDAP v2 protocol, which is defined in RFC 1777 [527]. RFC 2559 supersedes RFC 1778 [217].

The use of FTP and HTTP to distribute certificates is specified in RFC 2585 [213]. The DPD and DPV protocols for delegating certificate path discovery and validation are given in RFC 3379 [468]. Similar functionality to DPV and DPD is also supported by the *Simple Certificate Validation Protocol* (SCVP), specified in an Internet draft [397]. Despite its appearance in an Internet draft, SCVP has never been published in an RFC.

§13.6

OCSP is specified in RFC 2560 [434]. It is also specified in ISO/IEC 15945 [290]. The functioning of DVCS is specified in RFC 3029 [26].

SCVP [397], discussed above, provides functionality broadly similar to that provided by OCSP, but also incorporates functionality provided by DVD and DVP.

§13.7

The PKIX Certificate Policy and Certificate Management Framework was first published as RFC 2527 in 1999 [113]; this has now been superseded by RFC 3647 [114] published in November 2003.

The ABA digital signature guidelines [32], published in 1996, have been very influential in influencing the development of CPs and CPSs.

Chapter 10 of Ford and Baum [171] provides an excellent introduction to this subject.

Chapter 14

Trusted Third Parties

14.1 Definitions and basic properties

14.2 Standards for managing trusted third parties

14.3 TTP requirements

14.4 TTP architectures

14.5 Time-stamping authorities

14.6 Digital archiving authorities

14.7 Notes

§14.1 — §14.4

Several standards discuss the management of trusted third parties in some form or another. These include:

- the general ISO/IEC guideline on the use of trusted third parties, ISO/IEC TR 14516 [296], which is identical to the International Telecommunication Union recommendation, ITU-T X.842 [338],

- the IETF RFC on the management of time-stamping authorities, IETF RFC 3628 [469], which is identical to the European Telecommunications Standards Institute standard, ETSI TS 102023 [164],

- the ANSI standard on PKI policies [14],

- and the ISO/IEC information security management guidelines, ISO/IEC 17799 [284].

The ISO/IEC standard on information security management will be discussed in detail in Chapter 16.

Some people are uncomfortable with a TTP service provider's obligation to reveal confidential information to law enforcement agencies. This is a classic example of the debate between civil liberties groups and law enforcement agencies about the use of strong cryptographic primitives by criminals. This debate is well documented [140, 208] but is well outside the scope of this book!

§14.5

Time-stamping mechanisms are specified in two different places: ISO/IEC 18014 and IETF RFC 3161. The ISO/IEC 18014 standard has three parts: ISO/IEC 18014-1 [293] which describes the general principles of time-stamping, ISO/IEC

18014-2 [294] which describes three mechanisms for producing independent (i.e. unlinked) time-stamping tokens and ISO/IEC 18014-3 [306] which describes a mechanism for linking tokens. IETF RFC 3161 [21] describes a time-stamping mechanism that is similar to one of the mechanisms specified in ISO/IEC 18014-2.

These standards only describe the technical means by which time-stamps may be produced, but any use of a time-stamping authority must also be correctly managed. In particular, ISO/IEC 18014 recommends that a time-stamping authority should be managed according to the guidelines set down in ISO/IEC TR 14516 [296], whilst IETF RFC 3161 recommends that a time-stamping authority should be managed according to the guidelines in IETF RFC 3628 [469].

The specification of coordinated universal time is contained in ITU-R TF.460-6 [340].

One potential drawback with linking time-stamping tokens is that one must have copies all of the earlier time-stamps in order to verify the ordering. For example, if an entity wishes to verify that document A was stamped before document B, then that entity will have to have the time-stamp for document A, the time-stamp for document B, and all time-stamps that have been issued in between. The entity must then check that the time-stamps were issued one after the other and that each contains the hash-code of the previous time-stamp. This could be quite a time-intensive job and would undoubtedly involve storing a lot of unrelated time-stamping tokens!

Of course, the time-stamping authority is not forced to include the hash-code of the previous document in every time-stamping token. It is usually enough for a time-stamp to include the hash-code of the last time-stamp token that the time-stamping issued to that entity. That entity could then determine the ordering of time-stamps that they have been issued without needing to store lots of other tokens.

More information about time-stamps and time-stamping can be found in [96, 97, 198, 199].

Chapter 15

Cryptographic APIs

15.1   Introduction

15.2   Standards for crypto APIs

15.3   GSS-API

15.4   PKCS #11

15.5   Security issues

15.6   Notes

§15.1

There are many books, see for example [190], on using cryptography within Java, including Java GSS-API. There are also a significant number of books, e.g. [108, 480], covering the use and functionality of smart cards, which are essentially a special type of hardware security module. Thus some of the discussions on the interfaces offered by smart cards are also of relevance to crypto APIs.

§15.2

Version 2 update 1 of GSS-API is specified in RFC 2743 [392]. Previous versions of the GSS-API specification can be found in RFC 1508 [389] (version 1), and RFC 2078 [391] (version 2).

The current release of PKCS #11 is version 2.11 [492]. This and previous versions of the PKCS #11 specifications are available at:

> `http://www.rsasecurity.com/rsalabs/pkcs/index.html` .

The current version of the interface to the IBM 4758 hardware security module is specified in [219].

NIST FIPS Pub. 140-2 was released in 2001 [445]; the '2' in the title indicates that this is the second revision of FIPS 140. The two parts of the ISO banking standard for secure cryptographic devices, ISO 13491, were published in 1998 [261, 281].

§15.3

The current version of the GSS-API C bindings are specified in RFC 2744 [525], which supersedes RFC 1509 [524]. The parallel Java bindings are given in RFC 2853 [361].

The Kerberos v5 GSS-API mechanism is described in RFC 1964 [390]. Note that Kerberos v5 itself is specified in RFC 1510 [374] (for more details see Chapter 10). The SPKM mechanism is specified in RFC 2025 [18].

There are four other RFCs which relate to use of GSS-API. Two of these describe how GSS-API can be used to support specific functions. RFC 1961 [405] describes how GSS-API can be used to provide authentication for v5 of the SOCKS Protocol (itself specified in RFC 1928 [387]). SOCKS is designed to enable application layer protocols to traverse network firewalls. RFC 2203 [148] allows Remote Procedure Call (RPC) protocols to use GSS-API security services. The other two RFCs provide enhancements to the base GSS-API functionality. RFC 2478 [41] specifies a security negotiation mechanism for GSS-API. It enable GSS-API peers to determine whether their credentials share common cryptographic mechanism(s), and, if so, to invoke security context establishment for a selected common mechanism. This is most useful for applications using GSS-API implementations supporting multiple cryptographic mechanisms. RFC 2479 [20] extends GSS-API for applications requiring protection of a generic data unit (such as a file or message) in a 'connectionless' way. It is thus suitable for applications such as secure electronic mail where data needs to be protected without any on-line connection with the intended recipient(s) of that data.

§15.4

The current version (v2.11 revision 1) of PKCS #11 is specified in [492]. A detailed critique of PKCS #11 has been provided by Clulow [116].

§15.5

Clulow's 2003 Master's Thesis [115] contains descriptions of a number of possible crypto API vulnerabilities in commercial hardware security modules.

Attacks on the key management interface for recent versions of the IBM 4758 have been identified by Bond and Anderson [80, 81].

An example of unnecessary flexibility in a crypto API which enables an attack is described by Bond [82]. In this attack, PINs can be discovered much more efficiently than would normally be the case by the fact that a 'decimalisation table' (used in PIN verification computations) is a parameter to one of the API functions, although in practice the table is fixed (and hence does not need to be a parameter). This allows special 'false tables' to be offered to the API, permitting fast searches of the PIN space. The existence of such an attack has independently been observed by Clulow [115].

Problems with key control for MAC keys have been identified in [421, 423]. If the degree of truncation of the MAC is not bound securely to the key (which is not the case for Cryptoki or the IBM 4758 API) then this enables accelerated attacks on MAC functions.

Finally, certain possible attacks on partial computations for MACs have been identified [93], although it is not clear whether this is a problem to which existing crypto APIs are prone (since most such APIs are at least partially confidential).

Chapter 16

Other standards

16.1 Random bit generation

16.2 Prime number generation

16.3 Authenticated Encryption

16.4 Security modules

16.5 Standards for the use of biometric techniques

16.6 Information security management

16.7 Notes

§16.1

There are three standards that discuss the generation of random bit in a systematic and self contained way: IETF RFC 1750 [145], ISO/IEC 18031 [307] and ANSI X9.82 [16]. Of these, only the IETF RFC is currently available. Both ANSI X9.82 and ISO/IEC 18031 (currently at the CD stage) should be published in the next couple of years.

Whilst it is generally true that an NRBG based on a physical source needs specialist hardware to measure the source, this does not mean that the physical sources must themselves be new components. IETF RFC 1750 points out that many existing computer systems naturally contain phenomena that could be used as entropy sources. The standard suggests that audio input to a machine or the random fluctuations in the rotational speed of a disk drive could both be used as effective entropy sources, if hardware was put into place to measure the phenomena.

A large body of academic work has been published on the subject of deterministic random bit generators. For example, Yao [526] has shown that a random bit generator is secure (produces bits which are effectively unbiased and independent) if no attacker can determine the next bit of the RBG's output with probability significantly greater than $1/2$. A good, if somewhat technical, overview of this theory is given by Goldreich [178].

Examples of DRBGs include the use of a suitably secure block cipher in counter or output feedback mode (a proof that the CTR mode of operation provides suitably random output if the underlying block cipher is perfect is given by Bellare *et al.* [46]), the Micali-Schnorr generator [415, 416], and the Blum-Blum-Shub generator [76, 77]. Details of all of these deterministic random bit generators can be found in Menezes, van Oorschot and Vanstone [407].

The NIST statistical tests for random bit generators are currently available as NIST Special Publication 800-22 [446]. Code for these tests is also available on the NIST

website:

$$\text{http://csrc.nist.gov/rng/ .}$$

§16.2

The first attempt to produce some kind of standardised advice for choosing primes was probably the 1986 patent submitted by Hellman and Back (U.S. patent #4,633,036). This defined a cryptographically strong prime as a prime number p where

- $p - 1$ has a large prime factor r,
- $p + 1$ has a large prime factor s,
- $r - 1$ has a large prime factor r', and
- $s - 1$ has a large prime factor s'.

It was thought, at the time, that the product of two primes of this form would make an ideal RSA modulus. This advice has now been largely superseded, as it seems that suitably large randomly generated prime numbers will satisfy these conditions with overwhelming probability.

Both the ANSI X9 committee and the ISO/IEC JTC1 have recently been working on standards for prime number generation. These are ANSI X9.80 [15], released in 2001, and ISO/IEC 18032 [316], which is at FDIS stage and should be published early in 2005.

A discussion of the problems associated with the "add-two-and-test" method of using a probabilistic primality test to generate a prime number is given by Brandt [90].

Several primality tests are currently in use. These include the Miller-Rabin test [479], the Frobenius-Grantham test [194] and the Lehmann test [388]. These algorithms are all probabilistic and have (relatively small) error probabilities.

Recently, a new primality test has been proposed by Agarwal, Saxena and Kayal [27]. This paper is very interesting from a mathematical point of view, as it proposes a fast (using a mathematical definition of the word "fast"), deterministic method for testing the primality of a number. Unfortunately, even though the algorithm is mathematically classed as a "fast" algorithm, in practice the algorithm is very slow when compared to the probabilistic test mentioned above. Hence, it is not thought to be of practical use for generating primes for cryptographic applications.

Prime number generation algorithms that do not make use of primality tests include Maurer's algorithm [404] and the Shawe-Taylor algorithm [502].

§16.3

Whilst the problems of authenticated encryption, and, in particular, the order in which one should apply an encryption and MAC algorithm, have been discussed for many years, we have recently begun to see some formal analysis of the problem. Bellare and Namprempre [49] have analysed the problem to see what can be proven

about the various schemes, and have come to the conclusion that the Encrypt-then-MAC approach is best.

The idea of a signcryption scheme – an asymmetric scheme that acts as both an asymmetric encryption and digital signature scheme – was first introduced by Zheng [528]. Again, recent research has analysed the problem of signcryption from a "provable security" point of view. Papers by An [35] and An, Dodis and Rabin [37] have proposed security models that discuss the security properties that a signcryption scheme should have, and have also examined the question of whether it is possible to get this security just by signing and encrypting a message (in some order).

NIST are attempting to standardise a single mode of operation for a block cipher that provides authenticated encryption. Currently, a draft standard exists that contains the CCM mode [451]. This choice has been the subject of fierce debate. Much of the arguments for and against CCM mode are summarised on the relevant section of the NIST website:

<div align="center">

`http://csrc.nist.gov/CryptoToolkit/modes` .

</div>

The CCM mode of a block cipher has been proposed by Housley, Whiting and Ferguson [216] and is included in IETF RFC 3610 [522], IEEE 802.11i [222] and the draft NIST standard [451]. A proof of security for this mode was produced by Jonsson [357]. Despite this, it has been heavily criticised, particularly by Rogaway and Wagner [489].

The EAX mode was proposed by Bellare, Rogaway and Wagner [52] to provide an alternative to the CCM mode. Another alternative to CCM mode is the OCB mode of operation [487], which predates CCM mode by a year. However, this mode has the disadvantage of having been patented and has not been made freely available — instead it can be licensed under reasonable and non-discriminatory terms. A further alternative is AES Key Wrap mode, given in IETF RFC 3394 [495], but this does not seem to be a serious contender for inclusion in the NIST standard.

The work on the ISO/IEC standard on authenticated encryption, ISO/IEC 19772 [321] is at a very early stage. It is unclear which algorithms will be included in this standard. The first draft contains specifications for the CCM, OCB and AES Key Wrap modes of operation of a block cipher.

§16.4

The general security requirements for a security module that is to be used in the retail banking sector are described in ISO 13491-1 [261]. The second part of the standard, ISO 13491-2 [281], describes specific requirements for systems using magnetic card stripe systems (both requirements for the cards themselves, and the terminals which interact with them). It may be thought, since we have motivated the discussion of security modules via the ANSI key management framework [30, 238, 239, 240], that key management is the only function for which security modules are used in the financial sector. This is not true. ISO 13491-1 states that security modules can be "used to protect messages, cryptographic keys and other sensitive information used in a retail banking environment"; whilst ISO 13491-2 describes specific requirements not only for devices involved with PIN or key creation or manipulation, but also devices with MAC and digital signature functionality.

The main general standard on security (cryptographic) modules is NIST FIPS Pub. 140-2 [445]. The corresponding ISO/IEC standard that is being developed is ISO/IEC 19790 [322].

NIST also runs a certification service for FIPS 140-2 (and for the preceding standard, NIST FIPS Pub. 140-1 [438]). Vendors can submit security modules to the certification service, which will check whether the module achieves the claimed security level. At the time of writing (Spring 2004), the NIST Cryptographic Module Validation Programme (CMVP) had certified 374 products, with 111 more products under review. More information about the CMVP can be found at:

```
http://csrc.nist.gov/cryptval/  .
```

§16.5

Biometric identification and authentication is a huge topic and several books have been written on the subject. For more information on biometrics the reader is referred to Jain, Bolle and Pankanti [352] and Nanavati, Thieme and Nanavati [436]. This chapter concentrates on the work contained in the (published) ANSI X9.84 standard [17]. Other (draft) standards include the ISO/IEC 19792 standard [301] (work on which is at a very early stage), the BioAPI specification [62], the Common Biometric Exchange File Format [443] and the OASIS XCBF format standard [462].

It should be emphasised that the liveness of a biometric should be checked before the biometric measurement is trusted. There are cases where criminals have fooled fingerprint sensors using dead fingers that have forcibly been removed from the bodies of authorised personnel! More recently, Matsumoto *et al.* [400] have shown that it is often possible to fool fingerprint sensors by making false fingerprints from melted gummy bears! These "gummy" fingers have fooled both the biometric measurement system and the liveness test.

§16.6

The ISO/IEC standard on information security management, ISO/IEC 17799 [284], is based on the British Standard BS 7799-1 [94]. This standard consists of a series of guidelines for good information security management. A second part to this national standard, BS 7799-2 [95], deals with the certification that an organisation is compliant with BS 7799-1. ISO/IEC JTC1/SC27 are currently discussing the possibility of endorsing a version of BS 7799-2 as an international standard.

Chapter 17

Standards: the future

Appendix A

Tables of standards

In this appendix we provide tables of standards documents listed in numerical order. This should enable the reader, faced with just a standard number, to find out what the title of the standard is, and where it is discussed in this book.

A.1   3GPP standards

The Third Generation Partnership Project (3GPP) standards that are discussed in this book are given in Table A.1. These standards are published by ETSI.

3GPP standards are freely available from the 3GPP website:

<p align="center"><code>http://www.3gpp.org/</code></p>

Table A.1: 3GPP standards

3GPP no.	Title	Relevant chapter(s)	Ref. no.
TS 33.102	Security Architecture	12	[160]
TS 33.105	Cryptographic Algorithm Requirements	4	[153]
TS 35.201	Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 1: $f8$ and $f9$ Specification	4	[154]
TS 35.202	Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 2: KASUMI Specification	4	[155]
TS 35.205	Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions $f1$, $f1^*$, $f2$, $f3$, $f4$, $f5$ and $f5^*$; Document 1: General	12	[156]
TS 35.206	Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions $f1$, $f1^*$, $f2$, $f3$, $f4$, $f5$ and $f5^*$; Document 2: Algorithm Specification	12	[161]
TS 35.207	Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions $f1$, $f1^*$, $f2$, $f3$, $f4$, $f5$ and $f5^*$; Document 3: Implementors' Test Data	12	[157]
TS 35.208	Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions $f1$, $f1^*$, $f2$, $f3$, $f4$, $f5$ and $f5^*$; Document 4: Design Conformance Test Data	12	[158]
TS 35.909	Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions $f1$, $f1^*$, $f2$, $f3$, $f4$, $f5$ and $f5^*$; Document 5: Summary and results of design and evaluation	12	[159]
TS 55.216	Specification of the A5/3 Encryption Algorithm for GSM and ECSD, and the GEA3 Encryption Algorithm for GPRS; Document 1: A5/3 and GEA3 Specifications	4	[162]

A.2   ANSI standards

The ANSI standards discussed in this book are listed in Table A.2.

ANSI X9 standards are available (for purchase) from:

$$\texttt{http://webstore.ansi.org/}\ .$$

Table A.2: ANSI X series standards

ANSI no.	Title	Relevant chapter(s)	Ref. no.
X3.92	Data Encryption Algorithm	4	[34]
X3.106	American National Standard for Information Systems — Data Encryption Algorithm — Modes of Operation	5	[33]
X9.9	Financial institution message authentication (wholesale)	7	[2]
X9.17	Financial Institution Key Management (Wholesale)	11	[3, 10]
X9.19	Financial institution retail message authentication	7	[1]
X9.24	Retail Financial Services — Symmetric Key Management — Part 1: Using Symmetric Techniques	11, 12	[30]
X9.30.1	Public Key Cryptography for the Financial Services Industry — Part 1: The Digital Signature Algorithm (DSA)	8	[4]
X9.31	Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)	8, 16	[7]
X9.42	Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography	12, 16	[12]
X9.52	Triple Data Encryption Algorithm Modes of Operation	5	[28]
X9.55	Public Key Cryptography for the Financial Services Industry: Extensions to Public Key Certificates and Certificate Revocation Lists	13	[5]
X9.57	Public Key Cryptography for the Financial Services Industry: Certificate Management	13	[6]
X9.62	Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)	8	[8]
X9.63	Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Using Elliptic Curve Cryptography	12	[13]
X9.69	Framework for Key Management Extensions	12	[9]

ANSI no.	Title	Relevant chapter(s)	Ref. no.
X9.71	Keyed Hash Message Authentication Code	7	[11]
X9.79-1	Part 1: Public Key Infrastructure — Practices and Policy	13, 14	[14]
X9.80	Prime Number Generation, Primality Testing, and Primality Certificates	16	[15]
X9.82	Random Number Generation	16	[16]
X9.84	Biometric Information Management and Security for the Financial Services Industry	16	[17]

A.3   BSI standards

The BSI standards discussed in this book are listed in Table A.3.
Information about the BSI can be found on its website at:

$$\texttt{http://www.bsi-global.com/} \ .$$

BSI standards can also be purchased from the site.

Table A.3: BSI standards

BSI no.	Title	Relevant chapter(s)	Ref. no.
7799-1	Information technology. Code of practice for information security management	16	[94]
7799-2	Information security management. Specification with guidance for use	16	[95]

A.4   ETSI standards

ETSI standards that are included in this book are given in Table A.4.

For more information about ETSI and to (freely) download ETSI standards, visit:

`http://www.etsi.org/` .

Table A.4: ETSI standards

ETSI no.	Title	Relevant chapter(s)	Ref. no.
SR 002176	Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures	8	[163]
TS 102023	Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities	14	[164]

A.5 IEEE standards

The IEEE standards included in this book are detailed in Table A.5.

More information on IEEE standards can be found on the IEEE website:

http://standards.ieee.org/ .

IEEE standards are also available for purchase through this website.

Table A.5: IEEE standards

IEEE no.	Title	Relevant chapter(s)	Ref. no.
802.11i	IEEE Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems LAN/MAN — Specific Requirements — Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security	16	[222]
1363	IEEE Standard Specifications for Public-Key Cryptography	4, 8, 12	[221]
1363a	IEEE Standard Specifications for Public-Key Cryptography — Amendment 1: Additional Techniques	4, 8, 12	[223]
1363.1	IEEE Standard Specification for Public Key Cryptographic Techniques Based on Hard Problems over Lattices	4	
1363.2	IEEE Standard Specification for Password-Based Public Key Cryptographic Techniques	4, 12	

A.6   IETF requests for comments

The IETF Requests For Comments (RFCs) discussed in this book are listed in Table A.6 in ascending numerical order.

IETF RFCs are freely available from many places on the Internet, including the IETF homepage:

`http://www.ietf.org/` .

Table A.6: Internet RFCs

RFC no.	Title	Relevant chapter(s)	Ref. no.
791	DARPA Internet Program Protocol Specification	13	[220]
1035	Domain Names — Implementation and Specification	13	[430]
1118	The Hitchhikers Guide to the Internet	2	[378]
1305	Network Time Protocol (Version 3): Specification, Implementation and Analysis	10	[417]
1319	The MD2 message-digest algorithm	6	[362]
1320	The MD4 message-digest algorithm	6	[482]
1321	The MD5 message-digest algorithm	6	[483]
1422	Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management	13	[369]
1507	DASS: Distributed Authentication Security Service	10	[368]
1508	Generic Security Service Application Program Interface	15	[389]
1509	Generic Security Service API : C-bindings	15	[524]
1510	The Kerberos Network Authentication Service (V5)	10, 12, 15	[374]
1630	Universal Resource Identifiers in WWW	13	[56]
1704	On Internet authentication	10	[201]
1750	Randomness recommendations for security	16	[145]
1760	The S/KEY one-time password system	10	[200]
1777	Lightweight Directory Access Protocol	13	[527]
1778	The String Representation of Standard Attribute Syntaxes	13	[217]
1928	SOCKS Protocol Version 5	15	[387]
1961	GSS-API Authentication Method for SOCKS Version 5	15	[405]
1964	The Kerberos Version 5 GSS-API Mechanism	15	[390]
2025	The Simple Public-Key GSS-API Mechanism (SPKM)	15	[18]
2026	The Internet Standards Process – Revision 3	2	[89]
2030	Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI	10	[418]
2078	Generic Security Service Application Program Interface, Version 2	15	[391]

RFC no.	Title	Relevant chapter(s)	Ref. no.
2104	HMAC: Keyed-hashing for message authentication	7	[377]
2202	Test cases for HMAC-MD5 and HMAC-SHA-1	7	[109]
2203	RPCSEC_GSS Protocol Specification	15	[148]
2246	The TLS Protocol, Version 1.0	12	[137]
2314	PKCS #10: Certification Request Syntax v1.5	13	[363]
2315	PKCS #7: Certification Message Syntax v1.5	13	[364]
2409	The Internet Key Exchange (IKE)	12	[203]
2459	Internet X.509 Public Key Infrastructure: Certificate and CRL Profile	13	[212]
2478	The Simple and Protected GSS-API Negotiation Mechanism	15	[41]
2479	Independent Data Unit Protection Generic Security Service Application Program Interface (IDUP-GSS-API)	15	[20]
2510	Internet X.509 Public Key Infrastructure: Certificate Management Protocols	13	[22]
2511	Internet X.509 Certificate Request Message Format	13	[433]
2522	Photuris: Session-Key Management Protocol	12	[366]
2527	Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework	13	[113]
2528	Internet X.509 Public Key Infrastructure: Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates	13	[214]
2559	Internet X.509 Public Key Infrastructure: Operational Protocols — LDAPv2	13	[78]
2560	X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol — OCSP	13	[434]
2585	Internet X.509 Public Key Infrastructure: Operational Protocols: FTP and HTTP	13	[213]
2587	Internet X.509 Public Key Infrastructure: LDAPv2 Schema	13	[79]
2630	Cryptographic Message Syntax	13	[211]
2631	Diffie-Hellman Key Agreement Method	12	[481]

RFC no.	Title	Relevant chapter(s)	Ref. no.
2712	Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)	12	[406]
2743	Generic Security Service Application Program Interface Version 2, Update 1	15	[392]
2744	Generic Security Service API Version 2: C-bindings	15	[525]
2797	Certificate Management Messages over CMS	13	[435]
2853	Generic Security Service API Version 2: Java Bindings	15	[361]
2875	Diffie-Hellman Proof-of-Possession Algorithms	13	[473]
2986	PKCS #10: Certification Request Syntax Specification Version 1.7	13	[460]
2994	A Description of the MISTY1 Encryption Algorithm	4	[461]
3029	Internet X.509 Public Key Infrastructure: Data Validation and Certification Server Protocols	13	[26]
3039	Internet X.509 Public Key Infrastructure: Qualified Certificates Profile	8, 13	[494]
3075	XML-Signature Syntax and Processing	8	[147]
3161	Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)	14	[21]
3174	US Secure Hash Algorithm (SHA-1)	6	[146]
3279	Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile	13	[471]
3280	Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile	13	[215]
3281	An Internet Attribute Certificate Profile for Authorization	13	[165]
3379	Delegated Path Validation and Delegated Path Discovery Protocol Requirements	13	[468]
3394	Advanced Encryption Standard (AES) Key Wrap Algorithm	5	[495]
3610	Counter with CBC-MAC (CCM)	5, 16	[522]

RFC no.	Title	Relevant chapter(s)	Ref. no.
3628	Policy Requirements for Time-Stamping Authorities (TSAs)	14	[469]
3647	Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework	13	[114]

A.7   ISO standards

The ISO and ISO/IEC standards discussed in this book are listed in Table A.7. Note that, in the table, the title given is that of the most recent edition of the standard.

For more information about ISO, and to purchase ISO standards, visit the ISO website:

<div align="center">

`http://www.iso.ch/` .

</div>

ISO standards can also be purchased from ISO national member bodies, such as ANSI in the U.S. and BSI in the U.K.

Table A.7: ISO and ISO/IEC standards

ISO no.	Title	Relevant chapter(s)	Ref. no.
7498-1	Information technology — Open Systems Interconnection — Basic Reference Model — The Basic Model	3	[241]
7498-2	Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture	3	[227]
7498-4	Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 4: Management framework	3	[228]
8372	Information processing — Modes of operation for a 64-bit block cipher algorithm	5	[224]
8730	Banking — Requirements for message authentication (wholesale)	7	[230]
8731-1	Banking — Approved algorithm for message authentication — Part 1: DEA	7	[225]
8731-2	Banking — Approved algorithm for message authentication — Part 2: Message authenticator algorithm	7	[235]
8732	Banking — Key managemant (wholesale)	11, 12	[226]
9594-8	Information technology — Open Systems Interconnection — The Directory: Part 8: Public-key and attribute certificate frameworks	10, 13	[268, 289]
9796	Information technology — Security techniques — Digital signature scheme giving message recovery	8	[233]
9796-2	Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms	8	[295]
9796-3	Information technology — Security techniques — Digital signature schemes giving message recovery — Part 3: Discrete logarithm based mechanisms	8	[285, 310]
9797-1	Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher	5, 6, 7	[229, 242, 276]

ISO no.	Title	Relevant chapter(s)	Ref. no.
9797-2	Information technology — Security techniques — Message Authentication Codes (MACs) — Part 2: Mechanisms using a hash-function	7	[286]
9798-1	Information technology — Security techniques — Entity authentication — Part 1: General	10	[234, 260]
9798-2	Information technology — Security techniques — Entity authentication — Part 2: Mechanisms using symmetric encipherment algorithms	10	[243, 277]
9798-3	Information technology — Security techniques — Entity authentication — Part 3: Mechanisms using digital signature techniques	10	[244, 269]
9798-4	Information technology — Security techniques — Entity authentication — Part 4: Mechanisms using a cryptographic check function	10	[246, 278]
9798-5	IT security techniques — Entity authentication — Part 5: Mechanisms using zero knowledge techniques	10	[279, 318]
9798-6	IT security techniques — Entity authentication — Part 6: Mechanisms using manual data transfer	10	[315]
9807	Banking and related financial services — Requirements for message authentication (retail)	7	[231]
9979	Information technology — Security techniques — Procedures for the registration of cryptographic algorithms	4	[280]
10116	IT security techniques — Modes of operation for an n-bit block cipher	5	[232, 256, 311]
10118-1	Information technology — Security techniques — Hash-functions — Part 1: General	6	[282]

ISO no.	Title	Relevant chapter(s)	Ref. no.
10118-2	Information technology — Security techniques — Hash-functions — Part 2: Hash-functions using an n-bit block cipher	6	[283]
10118-3	Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions	6	[303]
10118-4	Information technology — Security techniques — Hash-functions — Part 4: Hash-functions using modular arithmetic	6	[262]
10181-1	Information technology — Open Systems Interconnection — Security frameworks for open systems — Part 1: Overview	3	[248]
10181-2	Information technology — Open Systems Interconnection — Security frameworks for open systems — Part 2: Authentication framework	3	[249]
10181-3	Information technology — Open Systems Interconnection — Security frameworks for open systems — Part 3: Access control framework	3	[250]
10181-4	Information technology — Open Systems Interconnection — Security frameworks for open systems — Part 4: Non-repudiation framework	3	[257]
10181-5	Information technology — Open Systems Interconnection — Security frameworks for open systems — Part 5: Confidentiality framework	3	[251]
10181-6	Information technology — Open Systems Interconnection — Security frameworks for open systems — Part 6: Integrity framework	3	[252]
10181-7	Information technology — Open Systems Interconnection — Security frameworks for open systems — Part 7: Security audit and alarms framework	3	[253]
10745	Information technology — Open Systems Interconnection — Upper layers security model	3	[245]

ISO no.	Title	Relevant chapter(s)	Ref. no.
11166-1	Banking — Key management by means of asymmetric algorithms — Part 1: Principles, procedures and formats	12	[236]
11166-2	Banking — Key management by means of asymmetric algorithms — Part 2: Approved algorithms using the RSA cryptosystem	12	[237]
11568-1	Banking — Key management (retail) — Part 1: Introduction to key management	11	[238]
11568-2	Banking — Key management (retail) — Part 2: Key management techniques for symmetric ciphers	11	[239]
11568-3	Banking — Key management (retail) — Part 3: Key life cycle for symmetric ciphers	11	[240]
11568-4	Banking — Key management (retail) — Part 4: Key management techniques using public key cryptosystems	11, 13	[263]
11568-5	Banking — Key management (retail) — Part 5: Key life cycle for public key cryptosystems	11, 13	[264]
11568-6	Banking — Key management (retail) — Part 6: Key management schemes	11	[270]
11770-1	Information technology — Security techniques — Key Management — Part 1: Framework	11	[254]
11770-2	Information technology — Security techniques — Key Management — Part 2: Mechanisms using symmetric techniques	12	[255]
11770-3	Information technology — Security techniques — Key Management — Part 3: Mechanisms using asymmetric techniques	12	[271]
11770-4	IT security techniques — Key Management — Part 4: Mechanisms based on weak secrets	12	[308]
13491-1	Banking — Secure cryptographic devices (retail) — Part 1: Concepts, requirements and evaluation methods	15, 16	[261]
13491-2	Banking — Secure cryptographic devices (retail) — Part 2: Security compliance checklists for devices used in magnetic stripe card systems	15, 16	[281]

ISO no.	Title	Relevant chapter(s)	Ref. no.
13594	Information technology — Lower layers security	3	[247]
13888-1	IT security techniques — Non-repudiation — Part 1: General	9	[258, 304]
13888-2	Information technology — Security techniques — Non-repudiation — Part 2: Mechanisms using symmetric techniques	9	[265]
13888-3	Information technology — Security techniques — Non-repudiation — Part 3: Mechanisms using asymmetric techniques	9	[259]
14516	Information technology — Security techniques — Guidelines for the use and management of Trusted Third Party services	14	[296]
14888-1	IT security techniques — Digital signatures with appendix — Part 1: General	8	[266]
14888-2	IT security techniques — Digital signatures with appendix — Part 2: Identity-based mechanisms	8	[272, 319]
14888-3	IT security techniques — Digital signatures with appendix — Part 3: Certificate-based mechanisms	8	[267, 320]
15408-1	Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model	3	[273]
15408-2	Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements	3	[274]
15408-3	Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements	3	[275]
15764	Road vehicles — Extended data link security	7	[302]

ISO no.	Title	Relevant chapter(s)	Ref. no.
15782-1	Certificate management for financial services — Part 1: Public key certificates	13	[298]
15782-2	Banking — Certificate management — Certificate extensions	13	[287]
15816	Information technology — Security techniques — Security information objects for access control	3	[288]
15945	Information technology — Security techniques — Specification of TTP services to support the application of digital signatures	13	[290]
15946-1	Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 1: General		
15946-2	Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 2: Digital signatures	8	[291]
15946-3	Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 3: Key establishment	12	
15946-4	Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 4: Digital signatures giving message recovery	8	[305]
15947	Information technology — Security techniques — IT intrusion detection framework	3	[297]
17799	Information technology — Code of practice for information security management	14, 16	[284]
18014-1	Information technology — Security techniques — Time-stamping services — Part 1: Framework	14	[293]
18014-2	Information technology — Security techniques — Time-stamping services — Part 2: Mechanisms producing independent tokens	14	[294]
18014-3	Information technology — Security techniques — Time-stamping services — Part 3: Mechanisms producing linked tokens	14	[306]
18031	IT security techniques — Random bit generation	16	[307]
18032	IT security techniques — Prime number generation	16	[316]
18033-1	IT security techniques — Encryption algorithms — Part 1: General	4	[317]

ISO no.	Title	Relevant chapter(s)	Ref. no.
18033-2	IT security techniques — Encryption algorithms — Part 2: Asymmetric ciphers	4	[312]
18033-3	IT security techniques — Encryption algorithms — Part 3: Block ciphers	4	[313]
18033-4	IT security techniques — Encryption algorithms — Part 4: Stream ciphers	4	[314]
19772	IT security techniques — Authenticated encryption mechanisms	5, 16	[321]
19790	Information technology — Security techniques — Security requirements for cryptographic modules	16	[322]
19792	Information technology — Security techniques — A framework for security evaluation and testing of biometric technology	16	[301]

A.8 ITU-T recommendations

The ITU-T Recommendations discussed in this book are listed in Table A.8.
More information about the ITU can be found on its website:

```
http://www.itu.int/ .
```

Further information on ITU-T standards can be found on a separate website:

```
http://www.itu.int/ITU-T/ .
```

Table A.8: ITU-T recommendations

ITU-T no.	Title	Relevant chapter(s)	Ref. no.
X.509	The directory — Public-key and attribute certificate frameworks	10, 13	[117, 324, 335, 336]
X.680	Information technology — Abstract Syntax Notation One ASN.1: Specification of basic notation	13	[341]
X.681	Information technology — Abstract Syntax Notation One ASN.1: Information object specification	13	[342]
X.682	Information technology — Abstract Syntax Notation One ASN.1: Constraint specification	13	[343]
X.683	Information technology — Abstract Syntax Notation One ASN.1: Parameterization of ASN.1 specifications	13	[344]
X.690	Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)	13	[345]
X.691	Information technology — ASN.1 encoding rules: Specification of Packed Encoding Rules (PER)	13	[346]
X.800	Data Communication Networks: Open Systems Interconnection (OSI); Security, Structure and Applications — Security Architecture for Open Systems Interconnection for CCITT Applications	3	[323, 333]
X.802	Data Networks and Open System Communications — Security — Information Technology — Lower Layers Security Model	3	[326]
X.803	Data Networks and Open System Communications — Security — Information Technology — Open Systems Interconnection — Upper Layers Security Model	3	[325]

ITU-T no.	Title	Relevant chapter(s)	Ref. no.
X.805	Security — Security architecture for systems providing end-to-end communications	3	[347]
X.810	Data Networks and Open System Communications — Security — Information Technology — Open Systems Interconnection — Security Frameworks for Open Systems: Overview	3	[327]
X.811	Data Networks and Open System Communications — Security — Information Technology — Open Systems Interconnection — Security Frameworks for Open Systems: Authentication Framework	3	[328]
X.812	Data Networks and Open System Communications — Security — Information Technology — Open Systems Interconnection — Security Frameworks for Open Systems: Access Control Framework	3	[329]
X.813	Data Networks and Open System Communications — Security — Information Technology — Open Systems Interconnection — Security Frameworks for Open Systems: Non-repudiation Framework	3	[334]
X.814	Data Networks and Open System Communications — Security — Information Technology — Open Systems Interconnection — Security Frameworks for Open Systems: Confidentiality Framework	3	[330]
X.815	Data Networks and Open System Communications — Security — Information Technology — Open Systems Interconnection — Security Frameworks for Open Systems: Integrity Framework	3	[331]
X.816	Data Networks and Open System Communications — Security — Information Technology — Open Systems Interconnection — Security Frameworks for Open Systems: Security Audit and Alarms Framework	3	[332]

ITU-T no.	Title	Relevant chapter(s)	Ref. no.
X.841	Security — Information technology — Security techniques — Security information objects for access control	3	[337]
X.842	Information technology — Security techniques — Guidelines for the use and management of Trusted Third Party services	14	[338]
X.843	Security — Information technology — Security techniques — Specification of TTP services to support the application of digital signatures	13	[339]

A.9 NIST FIPS

The NIST Federal Information Processing Standards (FIPS) that are discussed in this book are listed in Table A.9. Note that only the most recent editions are listed.

NIST FIPS can be freely downloaded from the NIST Computer Security Resource Center (CSRC) homepage at

```
http://csrc.nist.gov/ .
```

Table A.9: NIST FIPS

NIST FIPS no.	Title	Relevant chapter(s)	Ref. no.
46-3	Data Encryption Standard	4	[441]
81	DES Modes of Operation	5	[437]
140-2	Security Requirements for Cryptographic Modules	16	[445]
180-2	Secure Hash Standard	6	[448]
186-2	Digital Signature Standard	8	[442]
196	Entity Authentication Using Public Key Cryptography	10	[440]
197	Specification for the Advanced Encryption Standard (AES)	4	[444]
198	The Keyed-Hash Message Authentication Code (HMAC)	7	[449]

The NIST special publications are listed in Table A.10.

Table A.10: NIST Special Publications

NIST SP no.	Title	Relevant chapter(s)	Ref. no.
800-22	A statistical test suite for random and pseudorandom number generation for cryptographic applications	16	[446]
800-38A	Recommendation for Block Cipher Modes of Operation: Methods and Techniques	5	[447]
800-38B	Draft Recommendation for Block Cipher Modes of Operation: The RMAC Authentication Mode	7	[450]
800-38C	Draft Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality	5, 16	[451]

A.10   RSA PKCS

The RSA Public-Key Cryptography Standards (PKCS) that are discussed in this book are detailed in Table A.11.

These standards can be freely downloaded from:

`http://www.rsasecurity.com/rsalabs/pkcs/index.html` .

Table A.11: RSA PKCS standards

PKCS no.	Title	Relevant chapter(s)	Ref. no.
1	RSA Cryptography Standard	4	
3	Diffie-Hellman Key Agreement Standard	4, 12	
5	Password-Based Cryptography Standard	4	
7	Cryptographic Message Syntax Standard	13	
8	Private-Key Information Syntax Standard	4	
10	Certification Request Syntax Standard	13	
11	Cryptographic Token Interface Standard	15	[492]
13	Elliptic Curve Cryptography Standard	4	

A.11   SECG standards

The SECG has only produced two standards. These are listed in Table A.12.

More information about the SECG, and the two standards that it has produced, is available on the following website:

$$\texttt{http://www.secg.org/}\ .$$

Table A.12: SECG standards

SECG no.	Title	Relevant chapter(s)	Ref. no.
SEC 1	Elliptic curve cryptography	4	[510]
SEC 2	Recommended elliptic curve domain parameters	4	[511]

Bibliography

[1] Accredited Standards Committee X9 — Financial Services. *ANSI X9.19, Financial institution retail message authentication*, August 1986.

[2] Accredited Standards Committee X9 — Financial Services. *ANSI X9.9–1986 (revised), Financial institution message authentication (wholesale)*, April 1986.

[3] Accredited Standards Committee X9 — Financial Services. *ANSI X9.17, Financial Institution Key Management (Wholesale)*, 1995.

[4] Accredited Standards Committee X9 — Financial Services. *ANSI X9.30.1, Public Key Cryptography for the Financial Services Industry – Part 1: The Digital Signature Algorithm (DSA)*, 1997.

[5] Accredited Standards Committee X9 — Financial Services. *ANSI X9.55–1997, Public Key Cryptography for the Financial Services Industry: Extensions to Public Key Certificates and Certificate Revocation Lists*, 1997.

[6] Accredited Standards Committee X9 — Financial Services. *ANSI X9.57–1997, Public Key Cryptography for the Financial Services Industry: Certificate Management*, 1997.

[7] Accredited Standards Committee X9 — Financial Services. *ANSI X9.31, Digital Signatures Using Reversible Publis Key Cryptography for the Financial Services Industry (rDSA)*, 1998.

[8] Accredited Standards Committee X9 — Financial Services. *ANSI X9.62, Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*, 1998.

[9] Accredited Standards Committee X9 — Financial Services. *ANSI X9.69–1998, American National Standard for Financial Services: Framework for Key Management Extensions*, 1998.

[10] Accredited Standards Committee X9 — Financial Services. *ANSI X9 TG–26–1999, Technical Guideline: Managing Risk and Mitigation Planning: Withdrawal of ANSI X9.17, Financial Institution Key Management (Wholesale)*, 1999.

[11] Accredited Standards Committee X9 — Financial Services. *ANSI X9.71–2000, Keyed Hash Message Authentication Code*, 2000.

[12] Accredited Standards Committee X9 — Financial Services. *ANSI X9.42, Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography*, 2001.

[13] Accredited Standards Committee X9 — Financial Services. *ANSI X9.63, Public Key Cryptography for the Financial Services Industry, Key Agreement and Key Transport Using Elliptic Curve Cryptography*, 2001.

[14] Accredited Standards Committee X9 — Financial Services. *ANSI X9.79-1:2001, Part 1: Public Key Infrastructure — Practices and Policy*, 2001.

[15] Accredited Standards Committee X9 — Financial Services. *ANSI X9.80, Prime Number Generation, Primality Testing, and Primality Certificates*, 2001.

[16] Accredited Standards Committee X9 — Financial Services. *ANSI X9.82, Random Number Generation (Draft)*, 2003.

[17] Accredited Standards Committee X9 — Financial Services. *ANSI X9.84–2003, Biometric Information Management and Security for the Financial Services Industry*, 2003.

[18] C. Adams. *RFC 2025, The Simple Public-Key GSS-API Mechanism (SPKM)*. Internet Engineering Task Force, October 1996.

[19] C. Adams. Constructing symmetric ciphers using the CAST design procedure. *Designs, Codes and Cryptography*, 12:283–316, 1997.

[20] C. Adams. *RFC 2479, Independent Data Unit Protection Generic Security Service Application Program Interface (IDUP-GSS-API)*. Internet Engineering Task Force, December 1998.

[21] C. Adams, P. Cain, D. Pinkas, and R. Zuccherato. *RFC 3161, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*. Internet Engineering Task Force, August 2001.

[22] C. Adams and S. Farrell. *RFC 2510, Internet X.509 Public Key Infrastructure: Certificate Management Protocols*. Internet Engineering Task Force, March 1999.

[23] C. Adams, G. Krammer, S. Mister, and R. Zuccherato. On the security of key derivation functions. In K. Zhang and Y. Zheng, editors, *Proceedings of the Information Security Conference (ISC 2004)*, volume 3225 of *Lecture Notes in Computer Science*, pages 134–145. Springer-Verlag, 2004.

[24] C. Adams and S. Lloyd. *Understanding PKI: Concepts, Standards, and Deployment Considerations*. Addison-Wesley, 2nd edition, 2002.

[25] C. Adams and S. Lloyd. *Understanding PKI: Concepts, Standards and Deployment Considerations*. Addison-Wesley, 2nd edition, 2003.

[26] C. Adams, P. Sylvester, M. Zolotarev, and R. Zuccherato. *RFC 3029, Internet X.509 Public Key Infrastructure: Data Validation and Certification Server Protocols*. Internet Engineering Task Force, February 2001.

[27] M. Agrawal, N. Kayal, and Nitin Saxena. PRIMES is in P. Available from `http://www.cse.iitk.ac.in/news/primality.html`, 2002.

[28] American Bankers Association. *ANSI X9.52–1998, Triple Data Encryption Algorithm Modes of Operation*, 1998.

[29] American Bankers Association. *ANSI X9 TG–24–1999, Technical Guideline: Managing Risk and Migration Planning: Withdrawal of ANSI X9.9, Financial Iinstitution Message Authentication Codes (MAC) Wholesale*, 1999.

[30] American Bankers Association. *ANSI X9.24–2002, Retail Financial Services — Symmetric Key Management — Part 1: Using Symmetric Techniques*, 2002.

[31] American Bar Association. *Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce*, 1996. Available from `http://www.abanet.org/scitech/ec/isc/dsg.pdf`.

[32] American Bar Association, Information Security Committee, Section of Science and Technology. *Digital Signature Guidelines*, 1996.

[33] American National Standards Institute. *ANSI X3.106–1983, American National Standard for Information Systems — Data Encryption Algorithm — Modes of Operation*, 1983.

[34] American National Standards Institute. *ANSI INCITS 92–1981 (R1998), Data Encryption Algorithm (formerly ANSI X3.92–1981 (R1998))*, 1998.

[35] J. H. An. Authenticated encryption in the public-key setting: Security notions and analyses. Available from `http://eprint.iacr.org/2001/079`, 2001.

[36] J. H. An and M. Bellare. Constructing VIL-MACs from FIL-MACs: Message authentication under weakened assumptions. In M. J. Wiener, editor, *Advances in Cryptology — Crypto '99*, volume 1666 of *Lecture Notes in Computer Science*, pages 252–269. Springer-Verlag, 1999.

[37] J. H. An, Y. Dodis, and T. Rabin. On the security of joint signature and encryption. In L. Knudsen, editor, *Advances in Cryptology – Eurocrypt 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 83–107. Springer-Verlag, 2002.

[38] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, and T. Tokita. The 128-bit block cipher Camellia. *IEICE Transactions on Fundamentals*, E85-A:11–24, 2002.

[39] A. Arsenault and S. Turner. *Internet Draft draft-ietf-pkix-roadmap-09, Internet X.509 Public Key Infrastructure: Roadmap.* Internet Engineering Task Force, July 2002.

[40] T. Austin and D. Huaman. *PKI: A Wiley Brief.* John Wiley and Sons Inc., 2001.

[41] E. Baize and D. Pinkas. *RFC 2478, The Simple and Protected GSS-API Negotiation Mechanism.* Internet Engineering Task Force, December 1998.

[42] E. Barkan, E. Biham, and N. Keller. Instant ciphertext-only cryptanalysis of GSM encrypted communications. In D. Boneh, editor, *Advances in Cryptology – Crypto 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 600–616. Springer-Verlag, 2003.

[43] R. K. Bauer, T. A. Berson, and R. J. Feiertag. A key distribution protocol using event markers. *ACM Transactions on Computer Systems*, 1(3):249–255, August 1983.

[44] M. Bellare, R. Canetti, and H. Krawczyk. Keyed hash functions and message authentication. In N. Koblitz, editor, *Advances in Cryptology — Crypto '96*, volume 1109 of *Lecture Notes in Computer Science*, pages 1–15. Springer-Verlag, 1996.

[45] M. Bellare, R. Canetti, and H. Krawczyk. A modular approach to the design and analysis of authentication and key exchange protocols. In *30th ACM Symposium on the Theory of Computing*, pages 419–428. ACM Press, 1998.

[46] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway. A concrete security treatment of symmetric encryption. In *Proceedings of the 38th IEEE symposium on Foundations of Computer Science*, pages 394–403. IEEE, 1997.

[47] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway. Relations among notions of security for public-key encryption schemes. In H. Krawczyk, editor, *Advances in Cryptology – Crypto '98*, volume 1462 of *Lecture Notes in Computer Science*, pages 26–45. Springer-Verlag, 1998.

[48] M. Bellare, J. Kilian, and P. Rogaway. The security of the cipher block chaining message authentication code. In Y. G. Desmedt, editor, *Advances in Cryptology — Crypto '94*, volume 839 of *Lecture Notes in Computer Science*, pages 341–358. Springer-Verlag, 1994.

[49] M. Bellare and C. Namprempre. Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. In T. Okamoto, editor, *Advances in Cryptology – Asiacrypt 2000*, volume 1976 of *Lecture Notes in Computer Science*, pages 531–545. Springer-Verlag, 2000.

[50] M. Bellare and P. Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *Proc. of the First ACM Conference on Computer and Communications Security*, pages 62–73, 1993.

[51] M. Bellare and P. Rogaway. Entity authentication and key distribution. In D. R. Stinson, editor, *Advances in Cryptology — Crypto '93*, volume 773 of *Lecture Notes in Computer Science*, pages 232–249. Springer-Verlag, 1994.

[52] M. Bellare, P. Rogaway, and D. Wagner. The EAX mode of operation. In B. Roy and W. Meier, editors, *Proceedings of the 11th Workshop on Fast Software Encryption (FSE 2004)*, volume 3017 of *Lecture Notes in Computer Science*, pages 389–407. Springer-Verlag, 2004.

[53] S. M. Bellovin and M. Merritt. Limitations of the Kerberos authentication system. *ACM Computer Communication Review*, 20(5):119–132, October 1990.

[54] S. M. Bellovin and M. Merritt. Limitations of the Kerberos authentication system. In *Proceedings of the Usenix Winter 1991 Conference,*

Dallas, TX, USA, January 1991, pages 253–267. Usenix Association, 1991.

[55] S. Berkovits, S. Chokhani, J. A. Furlong, J. A. Geiter, and J. C. Guild. Public key infrastructure study: Final report, April 1994. National Institute of Standards and Techhnology.

[56] T. Berners-Lee. *RFC 1630, Universal Resource Identifiers in WWW*. Internet Engineering Task Force, June 1994.

[57] E. Biham and R. Chen. Near-collisions in SHA-0. In M. Franklin, editor, *Advances in Cryptology – Crypto 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 290–305. Springer-Verlag, 2004.

[58] E. Biham and L. R. Knudsen. Cryptanalysis of the ANSI X9.52 CBCM mode. In K. Nyberg, editor, *Advances in Cryptology — Eurocrypt '98*, volume 1403 of *Lecture Notes in Computer Science*, pages 100–111. Springer-Verlag, 1998.

[59] E. Biham and L. R. Knudsen. Cryptanalysis of the ANSI X9.52 CBCM mode. *Journal of Cryptology*, 15:47–59, 2002.

[60] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. In A. J. Menezes and S. A. Vanstone, editors, *Advances in Cryptology – Crypto '90*, volume 537 of *Lecture Notes in Computer Science*, pages 2–21, 1990.

[61] E. Biham and A. Shamir. Differential cryptanalysis of the full 16-round DES. In E. F. Brickell, editor, *Advances in Cryptology – Crypto '92*, volume 740 of *Lecture Notes in Computer Science*, pages 487–496. Springer-Verlag, 1992.

[62] The BioAPI Consortium. *BioAPI Specification Version 1.1*, March 2001.

[63] M. Bishop. *Computer Security: Art and Science*. Addison-Wesley, 2002.

[64] J. Black and P. Rogaway. CBC-MACs for arbitrary length messages: The three-key constructions. In M. Bellare, editor, *Advances in Cryptology — Crypto 2000*, volume 1880 of *Lecture Notes in Computer Science*, pages 197–215. Springer-Verlag, 2000.

[65] J. Black and P. Rogaway. A block-cipher mode of operation for parallelizable message authentication. In L. R. Knudsen, editor, *Advances in Cryptology — Eurocrypt 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 384–397. Springer-Verlag, 2002.

[66] J. Black, P. Rogaway, and T. Shrimpton. Black-box analysis of the block-cipher-based hash-function constructions form PGV. In M. Yung, editor, *Advances in Cryptology – Crypto 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 320–335. Springer-Verlag, 2002.

[67] J. Black and H. Urtubia. Side-channel attacks on symmetric encryption schemes: The case for authenticated encryption. In *Proceedings of the 11th USENIX Security Symposium, San Francisco, CA, USA, August 5-9, 2002*, pages 327–338. USENIX, 2002.

[68] I. Blake, G. Seroussi, and N. Smart. *Elliptic Curves in Cryptography*. Cambridge Univeristy Press, 1999.

[69] I. Blake, G. Seroussi, and N. Smart. *Elliptic Curves in Cryptography II: Further Topics*. Cambridge University Press, 2004. to appear.

[70] S. Blake-Wilson, D. Johnson, and A. Menezes. Key agreement protocols and their security analysis. In M. Darnell, editor, *Cryptography and Coding, 6th IMA International Conference*, volume 1355 of *Lecture Notes in Computer Science*, pages 30–45. Springer-Verlag, 1997.

[71] S. Blake-Wilson and A. Menezes. Entity authentication and authenticated key transport protocols employing asymmetric techniques. In B. Christianson, B. Crispo, T. M. A. Lomas, and M. Roe, editors, *Security Protocols, 5th International Workshop*, volume 1361 of *Lecture Notes in Computer Science*, pages 137–158. Springer-Verlag, 1998.

[72] G. R. Blakley. Safeguarding cryptographic keys. In *Proceedings of the National Computer Conference, 1979*, volume 48 of *American Federation of Information Processing Societies Proceedings*, pages 313–317, 1979.

[73] D. Bleichenbacher. Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS# 1. In H. Krawczyk, editor, *Advances in Cryptology – Crypto '98*, volume 1462 of *Lecture Notes in Computer Science*, pages 1–12. Springer-Verlag, 1998.

[74] D. Bleichenbacher. On the generation of DSA one-time keys. Lecture given at the 6th Workshop on Elliptic Curve Cryptography (ECC 2002), 2002.

[75] Bluetooth SIG. *Specification of the Bluetooth System*, 2004.

[76] L. Blum, M. Blum, and M. Shub. Comparison of two pseudo-random number generators. In D. Chaum, R. L. Rivest, and A. T. Sherman, editors, *Advances in Cryptology – Crypto '82*, pages 61–78. Plenum Publishing, 1982.

[77] L. Blum, M. Blum, and M. Shub. A simple unpredictable pseudo-random number generator. *SIAM Journal on Computing*, 15:364–383, 1986.

[78] S. Boeyen, T. Howes, and P. Richard. *RFC 2559, Internet X.509 Public Key Infrastructure: Operational Protocols — LDAPv2*. Internet Engineering Task Force, April 1999.

[79] S. Boeyen, T. Howes, and P. Richard. *RFC 2587, Internet X.509 Public Key Infrastructure: LDAPv2 Schema*. Internet Engineering Task Force, June 1999.

[80] M. Bond. Attacks on cryptoprocessor transaction sets. In C. K. Koc, D. Naccache, and C. Paar, editors, *Cryptographic Hardware and Embedded Systems — CHES 2001*, volume 2162 of *Lecture Notes in Computer Science*, pages 220–234. Springer-Verlag, 2001.

[81] M. Bond and R. Anderson. API-level attacks on embedded systems. *IEEE Computer Magazine*, 34(10):67–75, October 2001.

[82] M. Bond and P. Zielinski. Decimalisation attacks for PIN cracking, 2002. Preprint, Computer Laboratory, University of Cambridge.

[83] D. Boneh. Twenty years of attacks on the RSA cryptosystem. *Notices of the American Mathematical Society (AMS)*, 46(2):203–213, 1999.

[84] D. Boneh and M. Franklin. Identity based encryption from the Weil pairing. In J. Killian, editor, *Advances in Cryptology – Crypto 2001*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer-Verlag, 2001.

[85] A. Bosselaers and B. Preneel, editors. *Integrity Primitives for Secure Information Systems, Final RIPE Report of the RACE Integrity Primitives Evaluation*, volume 1007 of *Lecture Notes in Computer Science*. Springer-Verlag, 1995.

[86] C. Boyd. A class of flexible and efficient key management protocols. In *9th IEEE Computer Security Foundations Workshop*, pages 2–8. IEEE Computer Society Press, 1996.

[87] C. Boyd. Personal correspondance, 2004.

[88] C. A. Boyd and A. Mathuria. *Protocols for key establishment and authentication*. Springer-Verlag, 2003.

[89] S. Bradner. *RFC 2026, The Internet Standards Process – Revision 3*. Internet Engineering Task Force, October 1996.

[90] J. Brandt and I. Damgård. On generation of probable primes by incremental search. In E. F. Brickell, editor, *Advances in Cryptology – Crypto '92*, volume 740 of *Lecture Notes in Computer Science*, pages 358–370. Springer-Verlag, 1992.

[91] J. Brandt, I. Damgård, P. Landrock, and T. P. Pedersen. Zero-knowledge authentication scheme with secret key exchange (extended abstract). In S. Goldwasser, editor, *Advances in Cryptology — Crypto '88*, volume 403 of *Lecture Notes in Computer Science*, pages 583–588. Springer-Verlag, 1990.

[92] M. Briceno, I. Goldberg, and D. Wagner. A pedagogical implementation of the GSM A5/1 and A5/2 "voice privacy" encryption algorithms. Available from `http://cryptome.org/gsm-a512.htm`, 1999.

[93] K. Brincat and C. J. Mitchell. Key recovery atacks on MACs based on properties of cryptographic APIs. In B. Honary, editor, *Cryptography and Coding, 8th IMA International Conference*, volume 2260 of *Lecture Notes in Computer Science*, pages 63–72. Springer-Verlag, 2001.

[94] British Standards Institute (BSI). *BS 7799-1. Information technology. Code of practice for information security management*, 2000.

[95] British Standards Institute (BSI). *BS 7799-2. Information security management. Specification with guidance for use*, 2002.

[96] A. Buldas, P. Laud, H. Lipmaa, and J. Villemson. Time-stamping with binary linking schemes. In H. Krawczyk, editor, *Advances in Cryptology – Crypto '98*, volume 1462 of *Lecture Notes in Computer Science*, pages 486–501. Springer-Verlag, 1998.

[97] A. Buldas, H. Lipmaa, and B. Schoenmakers. Optimally efficient accountable time-stamping. In H. Imai and Y. Zheng, editors, *Public Key Cryptography 2000*, volume 1751 of *Lecture Notes in Computer Science*, pages 293–305. Springer-Verlag, 2000.

[98] M. Burmester. On the risk of opening distributed keys. In Y. Desmedt, editor, *Advances in Cryptology – Crypto '94*, volume 839 of *Lecture Notes in Computer Science*, pages 308–317. Springer-Verlag, 1994.

[99] W. E. Burr. Selecting the Advanced Encryption Standard. *IEEE Security and Privacy*, 1(2):43–52, March/April 2003.

[100] M. Burrows, M. Abadi, and R. Needham. Authentication: A practical study in belief and action. In M. Vardi, editor, *Proceedings of the Second Conference on Theoretical Aspects of Reasoning and Knowledge*, pages 325–342. Morgan Kaufmann, 1988.

[101] M. Burrows, M. Abadi, and R. Needham. A logic of authentication. *ACM Operating Systems Review*, 23(5):1–13, 1989.

[102] M. Burrows, M. Abadi, and R. Needham. A logic of authentication. *Proceedings of the Royal Society of London, Series A*, 426:233–271, 1989.

[103] M. Burrows, M. Abadi, and R. Needham. A logic of authentication. Technical Report 39, Digital Equipment Corporation Systems Research Center, February 1990. Revised version.

[104] C. M. Campbell Jr. Design and specification of cryptographic capabilities. In D. K. Branstad, editor, *NBS Special Publication 500-27: Computer security and the Data Encryption Standard*, pages 54–66. U.S. Department of Commerce, National Bureau of Standards, 1977.

[105] R. Canetti and H. Krawczyk. Analysis of key-exchange protocols and their use for building secure channels. In B. Pfitzmann, editor, *Advances in Cryptology – Eurocrypt 2001*, volume 2045 of *Lecture Notes in Computer Science*, pages 453–474. Springer-Verlag, 2001.

[106] B. Canvel, A. Hiltgen, S. Vaudenay, and M. Vuagnoux. Password interception in a SSL/TLS channel. In D. Boneh, editor, *Advances in Cryptology — CRYPTO 2003*, volume 2729 of *Lecture Notes in Computer Science*, pages 583–599. Springer-Verlag, Berlin, 2003.

[107] D. W. Chadwick. *Understanding X.500: The Directory.* Chapman and Hall, 1994.

[108] Z. Chen. *Java Card Technology for Smart Cards: Architecture and Programmer's Guide.* Addison-Wesley Longman Publishing Co., 2000.

[109] P. Cheng and R. Glenn. *RFC 2202, Test cases for HMAC-MD5 and HMAC-SHA-1.* Internet Engineering Task Force, September 1997.

[110] Z. Cheng and R. Comley. Attacks on an ISO/IEC 11770-2 key establishment protocol. Available from `http://eprint.iacr.org/2004/249/`, 2004.

[111] W. R. Cheswick, S. M. Bellovin, and A. D. Rubin. *Firewalls and Internet Security: Repelling the Wily Hacker.* Addison Wesley, 2nd edition, 2003.

[112] S. Chokhani. Toward a national public key infrastructure. *IEEE Communications Magazine*, 32(9):70–74, September 1994.

[113] S. Chokhani and W. Ford. *RFC 2527, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework.* Internet Engineering Task Force, March 1999.

[114] S. Chokhani, W. Ford, R. Sabett, C. Merrill, and S. Wu. *RFC 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework*. Internet Engineering Task Force, November 2003.

[115] J. Clulow. The design and analysis of cryptographic APIs for security devices, 2003. M.Sc. Dissertation, University of Natal, Durban, South Africa.

[116] J. Clulow. On the security of PKCS #11. In C. D. Walter, C. K. Koc, and C. Paar, editors, *Cryptographic Hardware and Embedded Systems — CHES 2003, 5th International Workshop*, volume 2779 of *Lecture Notes in Computer Science*, pages 411–425. Springer-Verlag, 2003.

[117] Comité Consultatif International de Télégraphique et Téléphonique. *CCITT Recommendation X.509 (1988), The directory — Authentication framework*, 1988.

[118] Committee on National Security Systems. *CNSS Policy No. 15, Fact Sheet No. 1: National Policy on the Use of the Advanced Encryption Standard (AES) to Protect National Security Systems and National Security Information*, June 2003. Available from `http://www.nstissc.gov/Assets/pdf/fact sheet.pdf`.

[119] D. Coppersmith, S. Halevi, and C. Jutla. ISO 9796-1 and the new forgery strategy. Available from `http://grouper.ieee.org/groups/1363/Research/Cryptanalysis.html`, 1999.

[120] D. Coppersmith, L. R. Knudsen, and C. J. Mitchell. Key recovery and forgery attacks on the MacDES MAC algorithm. In M. Bellare, editor, *Advances in Cryptology — Crypto 2000*, volume 1880 of *Lecture Notes in Computer Science*, pages 184–196. Springer-Verlag, 2000.

[121] D. Coppersmith and C. J. Mitchell. Attacks on MacDES MAC algorithm. *Electronics Letters*, 35:1626–1627, 1999.

[122] D. Coppersmith and A. Shamir. Lattice attacks on NTRU. In W. Fumy, editor, *Advances in Cryptology – Eurocrypt '97*, volume 1233 of *Lecture Notes in Computer Science*, pages 52–61. Springer-Verlag, 1997.

[123] J. S. Coron, D. Naccache, and J. P. Stern. On the security of RSA padding. In M. Weiner, editor, *Advances in Cryptology – Crypto '99*, volume 1666 of *Lecture Notes in Computer Science*, pages 1–18. Springer-Verlag, 1999.

[124] N. T. Courtois and J. Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations. In Y. Zheng, editor, *Advances in Cryptology – Asiacrypt 2002*, volume 2501 of *Lecture Notes in Computer Science*, pages 267–287. Springer-Verlag, 2002.

[125] M. Curtin and J. Dolske. A brute force seach of DES keyspace. *;login: – The Magazine of the USENIX Association*, May 1998. also available from `http://www.interhack.net/pubs/des-key-crack/`.

[126] I. B. Damgård. Collision free hash functions and public key signature schemes. In D. Chaum and W. L. Price, editors, *Advances in Cryptology – Eurocrypt '87*, volume 304 of *Lecture Notes in Computer Science*, pages 203–216. Springer-Verlag, 1987.

[127] I. B. Damgård. A design principle for hash functions. In G. Brassard, editor, *Advances in Cryptology – Crypto '89*, volume 435 of *Lecture Notes in Computer Science*, pages 416–427. Springer-Verlarg, 1989.

[128] E. Danielyan. Goodbye DES, welcome AES. *The Internet Protocol Journal*, 4(2):15–21, June 2001.

[129] J. Dankers, T. Garefalakis, R. Schaffelhofer, and T. Wright. PKI in mobile systems. In C. J. Mitchell, editor, *Security for Mobility*, chapter 2, pages 11–33. IEE, 2004.

[130] D. W. Davies. Some regular properties of the 'Data Encryption Standard' algorithm. In D. Chaum, R. L. Rivest, and A. T. Sherman, editors, *Advances in Cryptology – Crypto '82*, pages 89–96. Plenum Publishing, 1982.

[131] D. W. Davies. A message authenticator algorithm suitable for a mainframe computer. In G. R. Blakley and D. Chaum, editors, *Advances in Cryptology — Crypto '84*, volume 196 of *Lecture Notes in Computer Science*, pages 393–400. Springer-Verlag, 1985.

[132] D. W. Davies and S. Murphy. Pairs and triplets of DES S-boxes. *Journal of Cryptology*, 8:1–25, 1995.

[133] D. W. Davies and W. L. Price. *Security for Computer Networks*. John Wiley and Sons, Inc., 2nd edition, 1989.

[134] B. den Boer and A. Bosselaers. Collisions for the compression function of MD5. In T. Helleseth, editor, *Advances in Cryptology – Eurocrypt '93*, volume 765 of *Lecture Notes in Computer Science*, pages 293–304. Springer-Verlag, 1993.

[135] D. E. Denning and G. M. Sacco. Timestamps in key distribution protocols. *Communications of the ACM*, 24:533–536, 1981.

[136] Department of Defense (US). *DoD 5200.28-STD, Trusted Computer System Evaluation Criteria*, 1985.

[137] T. Dierks and C. Allen. *RFC 2246, The TLS Protocol, Version 1.0.* Internet Engineering Task Force, January 1999.

[138] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22:644–654, 1976.

[139] W. Diffie and M. E. Hellman. Privacy and authentication: An introduction to cryptography. *Proceedings of the IEEE*, 67:397–427, 1979.

[140] W. Diffie and S. Landau. *Privacy on the Line.* MIT Press, 1999.

[141] W. Diffie, P. C. van Oorschot, and M. J. Wiener. Authentication and authenticated key exchange. *Designs, Codes and Cryptography*, 2:107–125, 1992.

[142] H. Dobbertin. Cryptanalysis of MD4. In D. Gollmann, editor, *Fast Software Encryption, Third International Workshop*, volume 1039 of *Lecture Notes in Computer Science*, pages 71–82. Springer-Verlag, 1996.

[143] H. Dobbertin. The status of MD5 after a recent attack. *CryptoBytes*, 2(2):1–6, 1996.

[144] W. Doonan. *Internet Draft draft-ietf-cat-sskm-01, SPKM with Shared Secret Keys (SSKM).* Internet Engineering Task Force, 1999.

[145] D. Eastlake, S. Crocker, and J. Schiller. *RFC 1750, Randomness recommendations for security.* Internet Engineering Task Force, December 1994.

[146] D. Eastlake and P. Jones. *RFC 3174, US Secure Hash Algorithm (SHA-1).* Internet Engineering Task Force, September 2001.

[147] D. Eastlake, J. Reagle, and D. Solo. *RFC 3075, XML-Signature Syntax and Processing.* Internet Engineering Task Force, March 2001.

[148] M. Eisler, A. Chiu, and L. Ling. *RFC 2203, RPCSEC_GSS Protocol Specification.* Internet Engineering Task Force, September 1997.

[149] P. Ekdahl and T. Johansson. A new version of the stream cipher SNOW. In K. Nyberg and H. Heys, editors, *Selected Areas in Cryptography, 9th Annual International Workshop, SAC 2002*, volume 2595 of *Lecture Notes in Computer Science*, pages 47–61. Springer-Verlag, Berlin, 2003.

[150] EMVCo. *EMV2000: Integrated Circuit Card Specification for Paymewnt Systems: Book 2 — Security and Key Management*, December 2000.

[151] European Computer Manufacturers Association. *ECMA TR/46, Security in Open Systems: A Security Framework*, July 1988.

[152] European Parliament and the Council of the European Union. *Directive 1999/93/EC of the European Parliament and of the Council on a Community framework for electronic signatures*, 1999. Available from `http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.`

[153] European Telecommunications Standards Institute (ETSI). *3GPP TS 33.105, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Cryptographic Algorithm Requirements*, June 2001.

[154] European Telecommunications Standards Institute (ETSI). *3GPP TS 35.201, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 1: f8 and f9 Specification*, June 2002.

[155] European Telecommunications Standards Institute (ETSI). *3GPP TS 35.202, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 2: KASUMI Specification*, June 2002.

[156] European Telecommunications Standards Institute (ETSI). *3GPP TS 35.205, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentiction and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 1: General*, June 2002.

[157] European Telecommunications Standards Institute (ETSI). *3GPP TS 35.207, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentiction and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 3: Implementors' Test Data*, June 2002.

[158] European Telecommunications Standards Institute (ETSI). *3GPP TS 35.208, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP*

authentiction and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 4: Design Conformance Test Data, June 2002.

[159] European Telecommunications Standards Institute (ETSI). *3GPP TS 35.909, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentiction and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 5: Summary and results of design and evaluation*, May 2002.

[160] European Telecommunications Standards Institute (ETSI). *3GPP TS 33.102, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security architecture*, September 2003.

[161] European Telecommunications Standards Institute (ETSI). *3GPP TS 35.206, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentiction and key generation functions f1, f1*, f2, f3, f4, f5 and f5*; Document 2: Algorithm Specification*, June 2003.

[162] European Telecommunications Standards Institute (ETSI). *3GPP TS 55.216, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Specification of the A5/3 Encryption Algorithm for GSM and ECSD, and the GEA3 Encryption Algorithm for GPRS; Document 1: A5/3 and GEA3 Specifications*, September 2003.

[163] European Telecommunications Standards Institute (ETSI). *ETSI SR 002176, Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures*, March 2003.

[164] European Telecommunications Standards Institute (ETSI). *ETSI TS 102023, Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities*, January 2003.

[165] S. Farrell and R. Housley. *RFC 3281, An Internet Attribute Certificate Profile for Authorization*. Internet Engineering Task Force, April 2002.

[166] J. Feghhi, J. Feghhi, and P. Williams. *Digital Certificates: Applied Internet Security*. Addison-Wesley, 1999.

[167] D. F. Ferraiolo, D. R. Kuhn, and R. Chandramouli. *Role-Based Access Control*. Artech House, 2003.

[168] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In A. M. Odlyzko, editor, *Advances in Cryptology — Crypto '86*, volume 263 of *Lecture Notes in Computer Science*, pages 186–194. Springer-Verlag, 1987.

[169] S. Fluhrer and S. Lucks. Analysis of the E0 encryption system. In S. Vaudenay and A. Youssef, editors, *Selected Areas in Cryptography (SAC 2001)*, volume 2259 of *Lecture Notes in Computer Science*, pages 38–48. Springer-Verlag, 2001.

[170] W. Ford. *Computer Communications Security: Principles, Standard Protocols and Techniques*. PTR Prentice-Hall, 1994.

[171] W. Ford and M. S. Baum. *Secure Electronic Commerce*. Prentice-Hall PTR, 2nd edition, 2001.

[172] C. Gehrmann, C. J. Mitchell, and K. Nyberg. Manual authentication for wireless devices. *Cryptobytes*, 7(1):29–37, 2004.

[173] C. Gehrmann and K. Nyberg. Enhancements to Bluetooth baseband security. In *Proceedings of Nordsec 2001*, November 2001.

[174] C. Gehrmann and K. Nyberg. Security in personal area networks. In C. J. Mitchell, editor, *Security for Mobility*, chapter 9, pages 191–230. IEE, 2004.

[175] M. Girault. Hash-functions using modulo-n operations. In D. Chaum and W. L. Price, editors, *Advances in Cryptology – Eurocrypt '87*, volume 304 of *Lecture Notes in Computer Science*, pages 217–226. Springer-Verlag, 1987.

[176] M. Girault. Self-certified public keys. In D. W. Davies, editor, *Advances in Cryptology — Eurocrypt '91*, volume 547 of *Lecture Notes in Computer Science*, pages 490–497. Springer-Verlag, 1992.

[177] M. Girault and J.-C. Pailles. On-line / off-line RSA-like. In *Proceedings of WCC 2003*, 2003.

[178] O. Goldreich. *Foundations of Cryptography: Basic Tools*. Cambridge University Press, 2001.

[179] O. Goldreich. *Foundations of Cryptography: Basic Applications*. Cambridge University Press, 2004.

[180] O. Goldreich, S. Goldwasser, and S. Halevi. Public-key cryptosystems from lattice reduction problems. In B. Kaliski, editor, *Advances in Cryptology – Crypto '97*, volume 1294 of *Lecture Notes in Computer Science*, pages 165–179. Springer-Verlag, 1997.

[181] O. Goldreich, S. Goldwasser, and S. Micali. How to construct random functions. *Journal of the ACM*, 33(4):792–807, 1986.

[182] S. Goldwasser and S. Micali. Probabilistic encryption. *Journal of Computer and System Science*, 28:270–299, 1984.

[183] S. Goldwasser, S. Micali, and R. L. Rivest. A digital signature scheme secure against adaptive chosen message attacks. *SIAM Journal of Computing*, 17(2):281–308, April 1988.

[184] J. D. Golic. A weakness of the linear part of stream cipher MUGI. In B. Roy and W. Meier, editors, *Fast Software Encryption, 11th International Workshop, FSE 2004*, volume 3017 of *Lecture Notes in Computer Science*, pages 178–192. Springer-Verlag, Berlin, 2004.

[185] J. D. Golić, V. Bagini, and G. Morgari. Linear cryptanalysis of Bluetooth stream cipher. In L. Knudsen, editor, *Advances in Cryptology – Eurocrypt 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 238–255. Springer-Verlag, 2002.

[186] D. Gollmann. What do we mean by entity authentication? In *Proceedings: 1996 IEEE Symposium on Security and Privacy*, pages 46–54. IEEE Computer Society Press, 1996.

[187] D. Gollmann. *Computer Security*. John Wiley and Sons, 1999.

[188] L. Gong. A security risk of depending on synchonized clocks. *ACM Operating Systems Review*, 26(1):49–53, January 1992.

[189] L. Gong. Variations on the themes of message freshness and replay. In *Proceedings: Computer Security Foundations Workshop VI*, pages 131–136. IEEE Computer Society Press, June 1993.

[190] L. Gong, G. Ellison, and M. Dageforde. *Inside Java 2 Platform Security: Architecture, API Design, and Implementation*. Addison-Wesley, 2nd edition, 2003.

[191] Government of the United Kingdom. *Electronic Communications Act 2000*, 2000. Available from `http://www.hmso.gov.uk/acts/acts2000/20000007.htm`.

[192] Government of the United Kingdom. *Explanatory Notes to Electronic Communications Act 2000*, 2000. Available from `http://www.hmso.gov.uk/acts/en/2000en07.htm`.

[193] Government of the United States of America. *Electronic Signatures in Global and National Commerce Act*, 2000. Available from `http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_bills&docid=f:s761e`

[194] J. Grantham. A probable prime test with high confidence. *Journal of Number Theory*, 72:32–47, 1998.

[195] F. Grieu. A chosen message attack on the ISO/IEC 9796-1 signature scheme. In B. Preneel, editor, *Advances in Cryptology – Eurocrypt 2000*, volume 1233 of *Lecture Notes in Computer Science*, pages 70–80. Springer-Verlag, 2000.

[196] L. C. Guillou and J.-J. Quisquater. A practical zero-knowledge protocol fitted to security microprocessor minimizing both trasmission and memory. In C. G. Günther, editor, *Advances in Cryptology — Eurocrypt '88*, volume 330 of *Lecture Notes in Computer Science*, pages 123–128. Springer-Verlag, 1988.

[197] L. C. Guillou, M. Ugon, and J.-J. Quisquater. Cryptographic authentication protocols for smart cards. *Computer Networks*, 36:437–451, 2001.

[198] S. Haber and W. Stornetta. How to time-stamp a digital document. *Journal of Cryptography*, 3(2):99–111, 1991.

[199] S. Haber and W. Stornetta. Secure names for bit-strings. In *Proceedings of the 4th ACM Conference on Computer and Communications Security*, pages 28–35. ACM Press, 1997.

[200] N. Haller. *RFC 1760, The S/KEY one-time password system*. Internet Engineering Task Force, February 1995.

[201] N. Haller and R. Atkinson. *RFC 1704, On Internet authentication*. Internet Engineering Task Force, October 1994.

[202] D. Hankerson, A. J. Menezes, and S. Vanstone. *Guide to Elliptic Curve Cryptography*. Springer-Verlag, 2004.

[203] D. Harkins and D. Carrel. *RFC 2409, The Internet Key Exchange (IKE)*. Internet Engineering Task Force, November 1998.

[204] V. Hassler. X.500 and LDAP security: A comparative overview. *IEEE Network*, 13(6):54–64, November/December 1999.

[205] J. Henshall and S. Shaw. *OSI explained*. Ellis Horwood, 1988.

[206] M. Hermelin and K. Nyberg. Correlation properties of the Bluetooth combiner. In Joo Seok Song, editor, *Information Security and Cryptology (ISISC '99)*, volume 1787 of *Lecture Notes in Computer Science*, pages 17–29. Springer-Verlag, 1999.

[207] F. Hillebrand. *GSM and UMTS: The creation of global mobile communications*. John Wiley and Sons, Inc., 2001.

[208] L. J. Hoffman, editor. *Building in Big Brother*. Springer-Verlag, 1995.

[209] D. Hong, J.-S. Kang, B. Preneel, and H. Ryu. A concrete security analysis for 3GPP-MAC. In T. Johansson, editor, *Fast Software Encryption, 10th International Workshop, FSE 2003*, volume 2887 of *Lecture Notes in Computer Science*, pages 154–169. Springer-Verlag, 2003.

[210] G. Horng and C.-K. Hsu. Weakness in the Helsinki protocol. *Electronics Letters*, 34:354–355, 1998.

[211] R. Housley. *RFC 2630, Cryptographic Message Syntax*. Internet Engineering Task Force, June 1999.

[212] R. Housley, W. Ford, W. Polk, and D. Solo. *RFC 2459, Internet X.509 Public Key Infrastructure: Certificate and CRL Profile.* Internet Engineering Task Force, January 1999.

[213] R. Housley and P. Hoffman. *RFC 2585, Internet X.509 Public Key Infrastructure: Operational Protocols: FTP and HTTP*. Internet Engineering Task Force, May 1999.

[214] R. Housley and W. Polk. *RFC 2528, Internet X.509 Public Key Infrastructure: Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates*. Internet Engineering Task Force, March 1999.

[215] R. Housley, W. Polk, W. Ford, and D. Solo. *RFC 3280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile*. Internet Engineering Task Force, April 2002.

[216] R. Housley, D. Whiting, and N. Ferguson. Counter with CBC-MAC. Available from `http://csrc.nist.gov/CryptoToolkit/modes/proposedmodes/`, 2002.

[217] T. Howes, S. Kille, and W. Yeong. *RFC 1778, The String Representation of Standard Attribute Syntaxes*. Internet Engineering Task Force, March 1995.

[218] C. I'Anson and C.J. Mitchell. Security defects in CCITT recommendation X.509 — The directory authentication framework. *ACM Computer Communication Review*, 20(2):30–34, 1990.

[219] IBM. *PCI Cryptographic Processor: CCA Basic Services Reference and Guide, Release 2.41*, September 2003.

[220] Information Sciences Institute, University of Southern California. *RFC 791, DARPA Internet Program Protocol Specification.* Internet Engineering Task Force, September 1981.

[221] Institute of Electrical and Electronics Engineers, Inc. *IEEE Standard Specifications for Public-Key Cryptography*, 2000.

[222] Institute of Electrical and Electronics Engineers, Inc. *IEEE Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems – LAN/MAN Specific Requirements – Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security*, 2002.

[223] Institute of Electrical and Electronics Engineers, Inc. *IEEE Standard Specifications for Public-Key Cryptography – Amendment 1: Additional Techniques*, 2004.

[224] International Organization for Standardization. *ISO 8372: 1987, Information processing — Modes of operation for a 64-bit block cipher algorithm*, 1987.

[225] International Organization for Standardization. *ISO 8731–1: 1987, Banking — Approved algorithm for message authentication — Part 1: DEA*, 1987.

[226] International Organization for Standardization. *ISO/IEC 8732, Banking — Key management (wholesale)*, 1988.

[227] International Organization for Standardization. *ISO 7498–2: 1989, Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*, 1989.

[228] International Organization for Standardization. *ISO/IEC 7498–4: 1989, Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 4: Management framework*, 1989.

[229] International Organization for Standardization. *ISO/IEC 9797: 1989, Data cryptographic techniques — Data integrity mechanism using a cryptographic check function employing a block cipher algorithm*, December 1989.

[230] International Organization for Standardization. *ISO 8730: 1986, Banking — Requirements for message authentication (wholesale)*, 2nd edition, 1990.

[231] International Organization for Standardization. *ISO 9807, Banking and related financial services — Requirements for message authentication (retail)*, 1991.

[232] International Organization for Standardization. *ISO/IEC 10116: 1991, Information technology — Modes of operation for an n-bit block cipher algorithm*, 1991.

[233] International Organization for Standardization. *ISO/IEC 9796, Information technology — Security techniques — Digital signature scheme giving message recovery*, September 1991.

[234] International Organization for Standardization. *ISO/IEC 9798–1: 1991, Information technology — Security techniques — Entity authentication mechanisms — Part 1: General model*, 1991.

[235] International Organization for Standardization. *ISO 8731–2: 1992, Banking — Approved algorithm for message authentication — Part 2: Message authenticator algorithm*, 2nd edition, 1992.

[236] International Organization for Standardization. *ISO/IEC 11166–1, Banking — Key management by means of asymmetric algorithms — Part 1: Principles, procedures and formats*, 1994.

[237] International Organization for Standardization. *ISO/IEC 11166–2, Banking — Key management by means of asymmetric algorithms — Part 2: Approved algorithms using the RSA cryptosystem*, 1994.

[238] International Organization for Standardization. *ISO/IEC 11568–1, Banking — Key management (retail) — Part 1: Introduction to key management*, 1994.

[239] International Organization for Standardization. *ISO/IEC 11568–2, Banking — Key management (retail) — Part 2: Key management techniques for symmetric ciphers*, 1994.

[240] International Organization for Standardization. *ISO/IEC 11568–3, Banking — Key management (retail) — Part 3: Key life cycle for symmetric ciphers*, 1994.

[241] International Organization for Standardization. *ISO/IEC 7498–1: 1994, Information technology — Open Systems Interconnection — Basic Reference Model — The Basic Model*, 2nd edition, 1994.

[242] International Organization for Standardization. *ISO/IEC 9797: 1994, Information technology — Security techniques — Data integrity mechanism using a cryptographic check function employing a block cipher algorithm*, 2nd edition, 1994.

[243] International Organization for Standardization. *ISO/IEC 9798–2: 1994, Information technology — Security techniques — Entity authentication Mechanisms — Part 2: Entity authentication using symmetric techniques*, 1994.

[244] International Organization for Standardization. *ISO/IEC 9798–3: 1994, Information technology — Security techniques — Entity authentication mechanisms — Part 3: Entity authentication using a public key algorithm*, 1994.

[245] International Organization for Standardization. *ISO/IEC 10745: 1995, Information technology — Open Systems Interconnection — Upper layers security model*, 1995.

[246] International Organization for Standardization. *ISO/IEC 9798–4: 1995, Information technology — Security techniques — Entity authentication — Part 4: Mechanisms using a cryptographic check function*, 1995.

[247] International Organization for Standardization. *ISO/IEC TR 13594: 1995, Information technology — Lower layers security*, 1995.

[248] International Organization for Standardization. *ISO/IEC 10181–1: 1996, Information technology — Open Systems Interconnection — Security frameworks for open systems — Part 1: Overview*, 1996.

[249] International Organization for Standardization. *ISO/IEC 10181–2: 1996, Information technology — Open Systems Interconnection — Security frameworks for open systems — Part 2: Authentication framework*, 1996.

[250] International Organization for Standardization. *ISO/IEC 10181–3: 1996, Information technology — Open Systems Interconnection — Security frameworks for open systems — Part 3: Access control framework*, 1996.

[251] International Organization for Standardization. *ISO/IEC 10181–5: 1996, Information technology — Open Systems Interconnection — Security frameworks for open systems — Part 5: Confidentiality framework*, 1996.

[252] International Organization for Standardization. *ISO/IEC 10181–6: 1996, Information technology — Open Systems Interconnection — Security frameworks for open systems — Part 6: Integrity framework*, 1996.

[253] International Organization for Standardization. *ISO/IEC 10181–7: 1996, Information technology — Open Systems Interconnection — Security frameworks for open systems — Part 7: Security audit and alarms framework*, 1996.

[254] International Organization for Standardization. *ISO/IEC 11770–1, Information technology — Security techniques — Key Management — Part 1: Framework*, 1996.

[255] International Organization for Standardization. *ISO/IEC 11770–2, Information technology — Security techniques — Key Management — Part 2: Mechanisms using symmetric techniques*, 1996.

[256] International Organization for Standardization. *ISO/IEC 10116: 1997, Information technology — Security techniques — Modes of operation for an n-bit block cipher*, 2nd edition, 1997.

[257] International Organization for Standardization. *ISO/IEC 10181–4: 1997, Information technology — Open Systems Interconnection — Security frameworks for open systems — Part 4: Non-repudiation framework*, 1997.

[258] International Organization for Standardization. *ISO/IEC 13888–1: 1997, Information technology — Security techniques — Non-repudiation — Part 1: General*, 1997.

[259] International Organization for Standardization. *ISO/IEC 13888–3: 1997, Information technology — Security techniques — Non-repudiation — Part 3: Mechanisms using asymmetric techniques*, 1997.

[260] International Organization for Standardization. *ISO/IEC 9798–1: 1997, Information technology — Security techniques — Entity authentication — Part 1: General*, 2nd edition, 1997.

[261] International Organization for Standardization. *ISO 13491-1: 1998, Banking — Secure cryptographic devices (retail) — Part 1: Concepts, requirements and evaluation methods*, 1998.

[262] International Organization for Standardization. *ISO/IEC 10118–4, Information technology — Security techniques — Hash-functions — Part 4: Hash-functions using modular arithmetic*, 1998.

[263] International Organization for Standardization. *ISO/IEC 11568–4, Banking — Key management (retail) — Part 4: Key management techniques using public key cryptosystems*, 1998.

[264] International Organization for Standardization. *ISO/IEC 11568–5, Banking — Key management (retail) — Part 5: Key life cycle for public key cryptosystems*, 1998.

[265] International Organization for Standardization. *ISO/IEC 13888–2: 1998, Information technology — Security techniques — Non-repudiation — Part 2: Mechanisms using symmetric techniques*, 1998.

[266] International Organization for Standardization. *ISO/IEC 14888-1: 1998, Information technology — Security techniques — Digital signatures with appendix — Part 1: General*, 1998.

[267] International Organization for Standardization. *ISO/IEC 14888-3: 1998, Information technology — Security techniques — Digital signatures with appendix — Part 3: Certificate-based mechanisms*, 1998.

[268] International Organization for Standardization. *ISO/IEC 9594–8: 1998, Information technology — Open Systems Interconnection — The Directory: Part 8: Authentication framework*, 3rd edition, 1998.

[269] International Organization for Standardization. *ISO/IEC 9798–3: 1998, Information technology — Security techniques — Entity authentication — Part 3: Mechanisms using digital signature techniques*, 2nd edition, 1998.

[270] International Organization for Standardization. *ISO/IEC 11568–6, Banking — Key management (retail) — Part 6: Key management schemes*, 1999.

[271] International Organization for Standardization. *ISO/IEC 11770–3, Information technology — Security techniques — Key Management — Part 3: Mechanisms using asymmetric techniques*, 1999.

[272] International Organization for Standardization. *ISO/IEC 14888-2: 1999, Information technology — Security techniques — Digital signatures with appendix — Part 2: Identity-based mechanisms*, 1999.

[273] International Organization for Standardization. *ISO/IEC 15408–1: 1999, Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model*, 1999.

[274] International Organization for Standardization. *ISO/IEC 15408–2: 1999, Information technology — Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements*, 1999.

[275] International Organization for Standardization. *ISO/IEC 15408–3: 1999, Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements*, 1999.

[276] International Organization for Standardization. *ISO/IEC 9797–1, Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher*, 1999.

[277] International Organization for Standardization. *ISO/IEC 9798–2: 1999, Information technology — Security techniques — Entity authentication — Part 2: Mechanisms using symmetric encipherment algorithms*, 2nd edition, 1999.

[278] International Organization for Standardization. *ISO/IEC 9798–4: 1999, Information technology — Security techniques — Entity authentication — Part 4: Mechanisms using a cryptographic check function*, 2nd edition, 1999.

[279] International Organization for Standardization. *ISO/IEC 9798-5: 1999, Information technology — Security techniques — Entity authentication — Part 5: Mechanisms using zero knowledge techniques*, 1999.

[280] International Organization for Standardization. *ISO/IEC 9979, Information technology — Security techniques — Procedures for the registration of cryptographic algorithms*, 2nd edition, April 1999.

[281] International Organization for Standardization. *ISO 13491-2: 2000, Banking — Secure cryptographic devices (retail) — Part 2: Security compliance checklists for devices used in magnetic stripe card systems*, 2000.

[282] International Organization for Standardization. *ISO/IEC 10118–1, Information technology — Security techniques — Hash-functions — Part 1: General*, 2nd edition, 2000.

[283] International Organization for Standardization. *ISO/IEC 10118–2, Information technology — Security techniques — Hash-functions — Part 2: Hash-functions using an n-bit block cipher*, 2nd edition, 2000.

[284] International Organization for Standardization. *ISO/IEC 17799, Information technology — Code of practice for information security management*, 2000.

[285] International Organization for Standardization. *ISO/IEC 9796-3: 2000, Information technology — Security techniques — Digital signature schemes giving message recovery — Part 3: Discrete logarithm based mechanisms*, 2000.

[286] International Organization for Standardization. *ISO/IEC 9797–2, Information technology — Security techniques — Message Authentication Codes (MACs) — Part 2: Mechanisms using a hash-function*, 2000.

[287] International Organization for Standardization. *ISO 15782–2: 2001, Banking — Certificate management — Certificate extensions*, 2001.

[288] International Organization for Standardization. *ISO/IEC 15816: 2001, Information technology — Security techniques — Security information objects for access control*, 2001.

[289] International Organization for Standardization. *ISO/IEC 9594–8: 2001, Information technology — Open Systems Interconnection — The Directory: Part 8: Public-key and attribute certificate frameworks*, 4th edition, 2001.

[290] International Organization for Standardization. *ISO/IEC 15945: 2002, Information technology — Security techniques — Specification of TTP services to support the application of digital signatures*, 2002.

[291] International Organization for Standardization. *ISO/IEC 15946-2, Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 2: Digital signatures*, 2002.

[292] International Organization for Standardization. *ISO/IEC 15946, Information technology — Security techniques — Cryptographic Techniques based on Elliptic Curves*, 2002.

[293] International Organization for Standardization. *ISO/IEC 18014-1, Information technology — Security techniques — Time-stamping services — Part 1: Framework*, 2002.

[294] International Organization for Standardization. *ISO/IEC 18014-2, Information technology — Security techniques — Time-stamping services — Part 2: Mechanisms producing independent tokens*, 2002.

[295] International Organization for Standardization. *ISO/IEC 9796-2: 2002, Information technology — Security techniques — Digital signature schemes giving message recovery — Part 2: Integer factorization based mechanisms*, 2nd edition, 2002.

[296] International Organization for Standardization. *ISO/IEC TR 14516, Information technology — Security techniques — Guidelines for the use and management of Trusted Third Party services*, 2002.

[297] International Organization for Standardization. *ISO/IEC TR 15947: 2002, Information technology — Security techniques — IT intrusion detection framework*, 2002.

[298] International Organization for Standardization. *ISO 15782–1: 2003, Certificate management for financial services — Part 1: Public key certificates*, 2003.

[299] International Organization for Standardization. *ISO/IEC CD 9798–6, Information technology — Security techniques — Entity authentication — Part 6: Mechanisms using manual data transfer*, December 2003.

[300] International Organization for Standardization. *ISO/IEC FCD 18033–3, Information technology — Security techniques — Encryption Algorithms — Part 3: Block Ciphers*, 2003.

[301] International Organization for Standardization. *ISO/IEC WD 19792, Information technology — Security techniques — A Framework for Security Evaluation and Testing of Biometric Technology*, 2003.

[302] International Organization for Standardization. *ISO 15764: 2004, Road vehicles — Extended data link security*, 2004.

[303] International Organization for Standardization. *ISO/IEC 10118–3, Information technology — Security techniques — Hash-functions — Part 3: Dedicated hash-functions*, 3rd edition, 2004.

[304] International Organization for Standardization. *ISO/IEC 13888–1: 2004, IT security techniques — Non-repudiation — Part 1: General*, 2nd edition, 2004.

[305] International Organization for Standardization. *ISO/IEC 15946-4, Information technology — Security techniques — Cryptographic techniques based on elliptic curves — Part 4: Digital signatures giving message recovery*, 2004.

[306] International Organization for Standardization. *ISO/IEC 18014-3, Information technology — Security techniques — Time-stamping services — Part 3: Mechanisms producing linked tokens*, 2004.

[307] International Organization for Standardization. *ISO/IEC 4th CD 18031, IT Security techniques — Random bit generation*, June 2004.

[308] International Organization for Standardization. *ISO/IEC CD 11770– 4, IT Security techniques — Key Management — Part 4: Mechanisms based on weak secrets*, May 2004.

[309] International Organization for Standardization. *ISO/IEC CD 18031, Information technology — Security techniques — Random bit generation*, 2004.

[310] International Organization for Standardization. *ISO/IEC CD 9796- 3, IT Security techniques — Digital signature schemes giving message recovery — Part 3: Discrete logarithm based mechanisms*, 2nd edition, June 2004.

[311] International Organization for Standardization. *ISO/IEC FCD 10116, Information technology — Security techniques — Modes of operation for an n-bit block cipher*, 3rd edition, 2004.

[312] International Organization for Standardization. *ISO/IEC FCD 18033–2, IT security techniques — Encryption Algorithms — Part 2: Asymmetric Ciphers*, June 2004.

[313] International Organization for Standardization. *ISO/IEC FCD 18033–3, IT security techniques — Encryption Algorithms — Part 3: Block Ciphers*, May 2004.

[314] International Organization for Standardization. *ISO/IEC FCD 18033–4, IT security techniques — Encryption Algorithms — Part 4: Stream Ciphers*, June 2004.

[315] International Organization for Standardization. *ISO/IEC FCD 9798–6, IT security techniques — Entity authentication — Part 6: Mechanisms using manual data transfer*, June 2004.

[316] International Organization for Standardization. *ISO/IEC FDIS 18032, IT security techniques — Prime number generation*, June 2004.

[317] International Organization for Standardization. *ISO/IEC FDIS 18033–1, IT security techniques — Encryption Algorithms — Part 1: General*, July 2004.

[318] International Organization for Standardization. *ISO/IEC FDIS 9798–5, IT security techniques — Entity authentication — Part 5: Mechanisms using zero-knowledge techniques*, 2nd edition, June 2004.

[319] International Organization for Standardization. *ISO/IEC WD 14888-2, IT security techniques — Digital signatures with appendix — Part 2: Integer factorization based mechanisms*, 2nd edition, June 2004.

[320] International Organization for Standardization. *ISO/IEC WD 14888-3, IT security techniques — Digital signatures with appendix — Part 3: Discrete logarithm based mechanisms*, 2nd edition, June 2004.

[321] International Organization for Standardization. *ISO/IEC WD 19772: 2004, Information technology — Security techniques — Authenticated encryption mechanisms*, 2004.

[322] International Organization for Standardization. *ISO/IEC WD 19790, Information technology — Security techniques — Security requirements for cryptographic modules*, 2004.

[323] International Telecommunication Union. *CCITT Recommendation X.800 (1991), Data Communication Networks: Open Systems Interconnection (OSI); Security, Structure and Applications — Security Architecture for Open Systems Interconnection for CCITT Applications*, 1991.

[324] International Telecommunication Union. *ITU-T Recommendation X.509 (1993), The directory — Authentication framework*, 2nd edition, 1993.

[325] International Telecommunication Union. *ITU-T Recommendation X.803 (07/94), Data Networks and Open System Communications — Security — Information Technology — Open Systems Interconnection — Upper Layers Security Model*, 1994.

[326] International Telecommunication Union. *ITU-T Recommendation X.802 (04/95), Data Networks and Open System Communications — Security — Information Technology — Lower Layers Security Model*, 1995.

[327] International Telecommunication Union. *ITU-T Recommendation X.810 (11/95), Data Networks and Open System Communications — Security — Information Technology — Open Systems Interconnection — Security Frameworks for Open Systems: Overview*, 1995.

[328] International Telecommunication Union. *ITU-T Recommendation X.811 (04/95), Data Networks and Open System Communications — Security — Information Technology — Open Systems Interconnection — Security Frameworks for Open Systems: Authentication Framework*, 1995.

[329] International Telecommunication Union. *ITU-T Recommendation X.812 (11/95), Data Networks and Open System Communications — Security — Information Technology — Open Systems Interconnection — Security Frameworks for Open Systems: Access Control Framework*, 1995.

[330] International Telecommunication Union. *ITU-T Recommendation X.814 (11/95), Data Networks and Open System Communications — Security — Information Technology — Open Systems Interconnection — Security Frameworks for Open Systems: Confidentiality Framework*, 1995.

[331] International Telecommunication Union. *ITU-T Recommendation X.815 (11/95), Data Networks and Open System Communications — Security — Information Technology — Open Systems Interconnection — Security Frameworks for Open Systems: Integrity Framework*, 1995.

[332] International Telecommunication Union. *ITU-T Recommendation X.816 (11/95), Data Networks and Open System Communications — Security — Information Technology — Open Systems Interconnection — Security Frameworks for Open Systems: Security Audit and Alarms Framework*, 1995.

[333] International Telecommunication Union. *ITU-T Recommendation X.800 Amendment 1 (10/96), Security Architecture for Open Systems Interconnection for CCITT Applications — Amendment 1: Layer Two Security Service and Mechanisms for LANs*, 1996.

[334] International Telecommunication Union. *ITU-T Recommendation X.813 (10/96), Data Networks and Open System Communications — Security — Information Technology — Open Systems Interconnection — Security Frameworks for Open Systems: Non-repudiation Framework*, 1996.

[335] International Telecommunication Union. *ITU-T Recommendation X.509 (08/97), The directory — Authentication framework*, 3rd edition, 1997.

[336] International Telecommunication Union. *ITU-T Recommendation X.509 (03/2000), The directory — Public-key and attribute certificate frameworks*, 4th edition, 2000.

[337] International Telecommunication Union. *ITU-T Recommendation X.841 (10/2000), Security — Information technology — Security techniques — Security information objects for access control*, 2000.

[338] International Telecommunication Union. *ITU-T Recommendation X.842 (10/00), Information technology — Security techniques — Guidelines for the use and management of Trusted Third Party services*, October 2000.

[339] International Telecommunication Union. *ITU-T Recommendation X.843 (10/2000), Security — Information technology — Security techniques — Specification of TTP services to support the application of digital signatures*, 2000.

[340] International Telecommunication Union. *ITU-R Recommendation TF.460-6 (02/02), Standard frequency and time-signal emissions*, February 2002.

[341] International Telecommunication Union. *ITU-T Recommendation X.680 (07/02), Information technology — Abstract Syntax Notation One ASN.1: Specification of basic notation*, 2002.

[342] International Telecommunication Union. *ITU-T Recommendation X.681 (07/02), Information technology — Abstract Syntax Notation One ASN.1: Information object specification*, 2002.

[343] International Telecommunication Union. *ITU-T Recommendation X.682 (07/02), Information technology — Abstract Syntax Notation One ASN.1: Constraint specification*, 2002.

[344] International Telecommunication Union. *ITU-T Recommendation X.683 (07/02), Information technology — Abstract Syntax Notation One ASN.1: Parameterization of ASN.1 specifications*, 2002.

[345] International Telecommunication Union. *ITU-T Recommendation X.690 (07/02), Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*, 2002.

[346] International Telecommunication Union. *ITU-T Recommendation X.691 (07/02), Information technology — ASN.1 encoding rules: Specification of Packed Encoding Rules (PER)*, 2002.

[347] International Telecommunication Union. *ITU-T Recommendation X.805 (10/2003), Security — Security architecture for systems providing end-to-end communications*, 2003.

[348] T. Iwata and T. Kohno. New security proofs for the 3GPP confidentiality and integrity algorithms. In B. Roy and W. Meier, editors, *Proceedings of FSE 2004*, volume 3017 of *Lecture Notes in Computer Science*, pages 427–445. Springer-Verlag, 2004.

[349] T. Iwata and K. Kurosawa. OMAC: One-key CBC MAC. In T. Johansson, editor, *Fast Software Encryption, 10th International Workshop, FSE 2003*, volume 2887 of *Lecture Notes in Computer Science*, pages 129–153. Springer-Verlag, 2003.

[350] T. Iwata and K. Kurosawa. On the correctness of security proofs for the 3GPP confidentiality and integrity algorithms. In K. G. Paterson, editor, *Cryptography and Coding, 9th IMA International Conference*, volume 2898 of *Lecture Notes in Computer Science*, pages 306–318. Springer-Verlag, 2003.

[351] T. Iwata and K. Kurosawa. Stronger security bounds for OMAC, TMAC and XCBC. In T. Johansson and S. Maitra, editors, *Progress in Cryptology – Indocrypt 2003*, volume 2904 of *Lecture Notes in Computer Science*, pages 402–415. Springer-Verlag, 2003.

[352] A. Jain, R.. Bolle, and S. Pankanti, editors. *Biometrics: Personal Identification in Networked Society*. Kluwer Academic Press, 1999.

[353] M. Jakobsson. Method and apparatus for immunizing against offline dictionary attacks. U.S. Patent Application 60/283,996. Filed on 16th April 2001.

[354] M. Jakobsson and S. Wetzel. Security weaknesses in Bluetooth. In D. Naccache, editor, *Topics in Cryptology – CT-RSA 2001*, volume 2020 of *Lecture Notes in Computer Science*, pages 176–191. Springer-Verlag, 2001.

[355] M. Jakobsson and S. Wetzel. Security weaknesses in Bluetooth. In David Naccache, editor, *Topics in Cryptology — CT-RSA 2001*, volume 2020 of *Lecture Notes in Computer Science*, pages 176–191. Springer-Verlag, 2001.

[356] E. Jaulmes, A. Joux, and F. Valette. On the security of randomized CBC-MAC beyond the birthday paradox limit: A new construction. In J. Daemen and V. Rijmen, editors, *Proceedings of the 9th International Workshop on Fast Software Encryption (FSE 2002)*, volume 2365 of *Lecture Notes in Computer Science*, pages 237–251. Springer-Verlag, 2002.

[357] J. Jonsson. On the security of CTR + CBC-MAC. In K. Nyberg and H. M. Heys, editors, *Selected Areas in Cryptography (SAC 2002)*, volume 2595 of *Lecture Notes in Computer Science*, pages 76–93. Springer-Verlag, 2002.

[358] A. Joux. Multicollisions in iterated hash functions. applications to cascaded constructions. In M. Franklin, editor, *Advances in Cryptology – Crypto 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 306–316. Springer-Verlag, 2004.

[359] A. Joux, G. Poupard, and J. Stern. New attacks against standardized MACs. In T. Johansson, editor, *Fast Software Encryption, 10th International Workshop, FSE 2003*, volume 2887 of *Lecture Notes in Computer Science*, pages 170–181. Springer-Verlag, 2003.

[360] M. Just and S. Vaudenay. Authenticated multi-party key agreement. In K. Kim and T. Matsumoto, editors, *Advances in Cryptology – Asiacrypt '96*, volume 1163 of *Lecture Notes in Computer Science*, pages 36–49. Springer-Verlag, 1996.

[361] J. Kabat and M. Upadhyay. *RFC 2853, Generic Security Service API Version 2 : Java Bindings*. Internet Engineering Task Force, June 2000.

[362] B. Kaliski. *RFC 1319, The MD2 message-digest algorithm*. Internet Engineering Task Force, April 1992.

[363] B. Kaliski. *RFC 2314, PKCS #10: Certification Request Syntax v1.5.* Internet Engineering Task Force, October 1997.

[364] B. Kaliski. *RFC 2315, PKCS #7: Certification Message Syntax v1.5.* Internet Engineering Task Force, October 1997.

[365] J.-S. Kang, S. U. Shin, D. Hong, and O. Yi. Provable security of KASUMI and 3GPP encryption mode f8. In C. Boyd, editor, *Advances in Cryptology — Asiacrypt 2001*, volume 2248 of *Lecture Notes in Computer Science*, pages 255–271. Springer-Verlag, 2001.

[366] P. Karn and W. Simpson. *RFC 2522, Photuris: Session-Key Management Protocol.* Internet Engineering Task Force, March 1999.

[367] J. Katz and M. Yung. Unforgeable encruption and chosen ciphertext secure modes of operation. In B. Schneier, editor, *Fast Software Encryption, 7th International Workshop, FSE 2000*, volume 1978 of *Lecture Notes in Computer Science*, pages 284–299. Springer-Verlag, 2001.

[368] C. Kaufman. *RFC 1507, DASS: Distributed Authentication Security Service.* Internet Engineering Task Force, September 1993.

[369] S. Kent. *RFC 1422, Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management.* Internet Engineering Task Force, February 1993.

[370] L. R. Knudsen and T. Kohno. Analysis of RMAC. In T. Johansson, editor, *Fast Software Encryption, 10th International Workshop, FSE 2003*, volume 2887 of *Lecture Notes in Computer Science*, pages 182–191. Springer-Verlag, 2003.

[371] L. R. Knudsen and C. J. Mitchell. Analysis of 3gpp-MAC and two-key 3gpp-MAC. *Discrete Applied Mathematics*, 128:181–191, 2003.

[372] L. R. Knudsen and C. J. Mitchell. Partial key recovery attack against RMAC. *Journal of Cryptology*, to appear.

[373] L. R. Knudsen and B. Preneel. MacDES: MAC algorithm based on DES. *Electronics Letters*, **34**:871–873, 1998.

[374] J. Kohl and C. Neuman. *RFC 1510, The Kerberos Network Authentication Service (V5).* Internet Engineering Task Force, September 1993.

[375] L. M. Kohnfelder. Towards a practical public-key cryptosystem, 1978. B.Sc. thesis, Department of Electrical Engineering, MIT.

[376] W. Kou. *Networking Security and Standards*. Kluwer Academic Press, 1997.

[377] H. Krawczyk, M. Bellare, and R. Canetti. *RFC 2104, HMAC: Keyed-hashing for message authentication*. Internet Engineering Task Force, February 1997.

[378] E. Krol. *RFC 1118, The Hitchhikers Guide to the Internet*. Internet Engineering Task Force, September 1989.

[379] K. Kurosawa and T. Iwata. TMAC: Two-key CBC MAC. In M. Joye, editor, *Topics in Cryptology — CT-RSA 2003*, volume 2612 of *Lecture Notes in Computer Science*, pages 33–49. Springer-Verlag, 2003.

[380] K.-Y. Lam. Building an authentication service for distributed systems. *Journal of Computer Security*, 1:73–84, 1993.

[381] L. Lamport. Time, clocks, and the ordering of events in a distributed system. *Communications of the ACM*, 21:558–565, 1978.

[382] L. Lamport. Password authentication with insecure communication. *Communications of the ACM*, 24:770–772, 1981.

[383] J. Larmouth. *ASN.1 Complete*. Morgan Kaufmann, 1999.

[384] J.-O. Larsson. Higher layer key exchange techniques for Bluetooth security. Open Group Conference, Amsterdam, October 2001.

[385] L. Law, A. Menezes, M. Qu, J. Solinas, and S. Vanstone. An efficient protocol for authenticated key agreement. *Designs, Codes and Cryptography*, 28(2):119–134, 2003.

[386] Law Commission. *Electronic Commerce: Formal Requirements in Commercial Transactions*, 2001.

[387] M. Leech, M. Ganis, Y. Lee, R. Kuris, D. Koblas, and L. Jones. *RFC 1928, SOCKS Protocol Version 5*. Internet Engineering Task Force, March 1996.

[388] D. J. Lehmann. On primality tests. *SIAM Journal of Computing*, 11(9):374–375, 1982.

[389] J. Linn. *RFC 1508, Generic Security Service Application Program Interface*. Internet Engineering Task Force, September 1993.

[390] J. Linn. *RFC 1964, The Kerberos Version 5 GSS-API Mechanism*. Internet Engineering Task Force, June 1996.

[391] J. Linn. *RFC 2078, Generic Security Service Application Program Interface, Version 2*. Internet Engineering Task Force, January 1997.

[392] J. Linn. *RFC 2743, Generic Security Service Application Program Interface Version 2, Update 1.* Internet Engineering Task Force, January 2000.

[393] G. Lowe. An attack on the Needham-Schroeder public-key authentication protocol. *Information Processing Letters*, 56:131–133, 1995.

[394] G. Lowe. Breaking and fixing the Needham-Schroeder public-key protocol using FDR. In T. Margaria and B. Steffen, editors, *Tools and Algorithms for Construction and Analysis of Systems, Second International Workshop, TACAS '96*, volume 1055 of *Lecture Notes in Computer Science*, pages 147–166. Springer-Verlag, 1996.

[395] Y. Lu and S. Vaudenay. Faster correlation attack on Bluetooth keystream generator E0. In M. Franklin, editor, *Advances in Cryptology – Asiacrypt 2004*, volume 3152 of *Lecture Notes in Computer Science*, pages 407–425. Springer-Verlag, 2004.

[396] D. P. Maher. Secure communication method and apparatus. U.S. Patent Number 5,450,493, September 1995. Filed on 29th December 1993.

[397] A. Malpani, R. Housley, and T. Freeman. *Internet Draft draft-ietf-pkix-scvp-13, Simple Certificate Validation Protocol.* Internet Engineering Task Force, October 2003.

[398] M. Matsui. Linear cryptanalysis method for DES cipher. In T. Helleseth, editor, *Advances in Cryptology – Eurocrypt '93*, volume 765 of *Lecture Notes in Computer Science*, pages 386–397. Springer-Verlag, 1993.

[399] M. Matsui. New block encryption algorithm MISTY. In E. Biham, editor, *Fast Software Encryption - 4th International Workshop (FSE '97)*, volume 1267 of *Lecture Notes in Computer Science*, pages 54–68. Springer-Verlag, 1997.

[400] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino. Impact of artificial "gummy" fingers on fingerprint systems. In R. L. van Renesse, editor, *Optical Security and Counterfeit Deterrence Techniques IV – Proceedings of SPIE, Volume 4677*, pages 275–289, 2002.

[401] T. Matsumoto, Y. Takashima, and H. Imai. On seeking smart public-key-distribution schemes. *Transactions of the IECE of Japan*, E69(2):99–106, 1986.

[402] S. M. Matyas. Key processing with control vectors. *Journal of Cryptology*, 3:113–116, 1991.

[403] S. M. Matyas, C. H. Meyer, and J. Oseas. Generating strong one-way functions with cryptographic algorithms. *IBM Technical Disclosure Bulletin*, 27:5658–5659, 1985.

[404] U. Maurer. Fast generation of prime numbers and secure public-key cryptographic parameters. *Journal of Cryptography*, 8:123–155, 1995.

[405] P. McMahon. *RFC 1961, GSS-API Authentication Method for SOCKS Version 5*. Internet Engineering Task Force, June 1996.

[406] A. Medvinsky and M. Hur. *RFC 2712, Addition of Kerberos Cipher Suites to Transport Layer Security (TLS)*. Internet Engineering Task Force, October 1999.

[407] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1997.

[408] R. C. Merkle. Secrecy, authentication and public key systems. Technical Report 1979-1, Information Systems Laboratory, Stanford University, 1979.

[409] R. C. Merkle. *Secrecy, Authentication and Public Key Systems*. UMI Research Press, 1982.

[410] R. C. Merkle. One way hash functions and DES. In G. Brassard, editor, *Advances in Cryptology – Crypto '89*, volume 435 of *Lecture Notes in Computer Science*, pages 428–446. Springer-Verlag, 1989.

[411] R. C. Merkle. A fast software one-way hash function. *Journal of Cryptology*, 3:43–58, 1990.

[412] C. H. Meyer and S. M. Matyas. *Cryptography: A new dimension in computer data security*. John Wiley and Sons, 1982.

[413] C. H. Meyer and M. Schilling. Secure program load with manipulation detection code. In *Proceedings of the 6th Worldwide Congress on Computer and Communication Security and Protection (SECURICOM '88)*, pages 111–130, 1988.

[414] S. Micali, C. Rackoff, and B. Sloan. The notion of security for probabilistic cryptosystems. *SIAM Journal on Computing*, 17:412–426, 1988.

[415] S. Micali and C. P. Schnorr. Efficient, perfect random number generators. In S. Goldwasser, editor, *Advances in Cryptology – Crypto '88*, volume 403 of *Lecture Notes in Computer Science*, pages 173–198. Springer-Verlag, 1988.

[416] S. Micali and C. P. Schnorr. Efficient, perfect polynomial random number generators. *Journal of Cryptography*, 3:157–172, 1991.

[417] D. L. Mills. *RFC 1305, Network Time Protocol (Version 3): Specification, Implementation and Analysis.* Internet Engineering Task Force, March 1992.

[418] D. L. Mills. *RFC 2030, Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI.* Internet Engineering Task Force, October 1996.

[419] D. L. Mills. *Internet Draft draft-ietf-stime-ntpauth-04, Public Key Cryptography for the Network Time Protocol: Version 2.* Internet Engineering Task Force, November 2002.

[420] C. J. Mitchell. Limitations of challenge-response entity authentication. *Electronics Letters*, 25:1195–1196, 1989.

[421] C. J. Mitchell. Key recovery attack on ANSI retail MAC. *Electronics Letters*, 39:361–362, 2003.

[422] C. J. Mitchell. On the security of XCBC, TMAC and OMAC. Technical Report RHUL-MA-2003-4, Mathematics Department, Royal Holloway, University of London, August 2003.

[423] C. J. Mitchell. Truncation attacks on MACs. *Electronics Letters*, 39:1439–1440, 2003.

[424] C. J. Mitchell. *Security for Mobility.* Institution of Electrical Engineers, 2004.

[425] C. J. Mitchell and L. Chen. Comments on the S/KEY user authentication scheme. *ACM Operating Systems Review*, 30(4):12–16, October 1996.

[426] C. J. Mitchell and R. Schaffelhofer. The personal PKI. In C. J. Mitchell, editor, *Security for Mobility*, chapter 3, pages 35–61. IEE, 2004.

[427] C. J. Mitchell and V. Varadharajan. Modified forms of cipher block chaining. *Computers and Security*, 10:37–40, 1991.

[428] C. J. Mitchell, M. Ward, and P. Wilson. On key control in key agreement protocols. *Electronics Letters*, 34:980–981, 1998.

[429] C. J. Mitchell and C. Y. Yeun. Fixing a problem in the Helsinki protocol. *ACM Operating Systems Review*, 32(4):21–24, October 1998.

[430] P. Mockapetris. *RFC 1035, Domain Names — Implementation and Specification.* Internet Engineering Task Force, November 1987.

[431] Frédéric Muller. The MD2 hash function is not one-way. In P. J. Lee, editor, *Advances in Cryptology – Asiacrypt 2004*, volume 3329 of *Lecture Notes in Computer Science*, pages 214–229. Springer-Verlag, 2004.

[432] S. Murphy and M. Robshaw. Essential algebraic structure within the AES. In M. Yung, editor, *Advances in Cryptology – Crypto 2002*, volume 2442 of *Lecture Notes in Computer Science*, pages 1–16. Springer-Verlag, 2002.

[433] M. Myers, C. Adams, D. Solo, and D. Kemp. *RFC 2511, Internet X.509 Certificate Request Message Format.* Internet Engineering Task Force, March 1999.

[434] M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams. *RFC 2560, X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol — OCSP.* Internet Engineering Task Force, June 1999.

[435] M. Myers, X. Liu, J. Schaad, and J. Weinstein. *RFC 2797, Certificate Management Messages over CMS.* Internet Engineering Task Force, April 2000.

[436] S. Nanavati, M. Thieme, and R. Nanavati. *Biometrics: Identity Verification in a Networked World.* John Wiley and Sons, Inc., 2002.

[437] National Institute of Standards and Technology (NIST). *Federal Information Processing Standards Publication 81 (FIPS PUB 81): DES Modes of Operation*, December 1980.

[438] National Institute of Standards and Technology (NIST). *Federal Information Processing Standards Publication 140-1 (FIPS PUB 140-1): Security Requirements for Cryptographic Modules*, January 1994.

[439] National Institute of Standards and Technology (NIST). *Proceedings: Public Key Infrastructure Invitational Workshop, MITRE, McLean, Virginia, USA*, September 1995. IR 5788.

[440] National Institute of Standards and Technology (NIST). *Federal Information Processing Standards Publication 196 (FIPS PUB 196): Entity authentication using public key cryptography*, February 1997.

[441] National Institute of Standards and Technology (NIST). *Federal Information Processing Standards Publication 46-3 (FIPS PUB 46-3): Data Encryption Standard*, October 1999.

[442] National Institute of Standards and Technology (NIST). *Federal Information Processing Standards Publication 186-2 (FIPS PUB 186-2): Digital Signature Standard (DSS)*, January 2000.

[443] National Institute of Standards and Technology (NIST). *Common Biometric Exchange File Format (CBEFF)*, January 2001.

[444] National Institute of Standards and Technology (NIST). *Federal Information Processing Standards Publication 197 (FIPS PUB 197): Specification for the Advanced Encryption Standard (AES)*, November 2001.

[445] National Institute of Standards and Technology (NIST). *Federal Information Processing Standards Publication 140-2 (FIPS PUB 140-2): Security Requirements for Cryptographic Modules*, June 2001.

[446] National Institute of Standards and Technology (NIST). *NIST Special Publication 800-22: A statistical test suite for random and pseudorandom number generation for cryptographic applications*, May 2001.

[447] National Institute of Standards and Technology (NIST). *NIST Special Publication 800-38A, Recommendation for Block Cipher Modes of Operation: Methods and Techniques*, December 2001.

[448] National Institute of Standards and Technology (NIST). *Federal Information Processing Standards Publication 180-2 (FIPS PUB 180-2): Secure Hash Standard*, August 2002.

[449] National Institute of Standards and Technology (NIST). *Federal Information Processing Standards Publication 198 (FIPS PUB 198): The Keyed-Hash Message Authentication Code (HMAC)*, March 2002.

[450] National Institute of Standards and Technology (NIST). *NIST Special Publication 800-38B, Draft recommendation for block cipher modes of operation: The RMAC authentication mode*, October 2002.

[451] National Institute of Standards and Technology (NIST). *NIST Special Publication 800-38C, Draft Recommendation for Block Cipher Modes of Operation: The CCM Mode For Authentication and Confidentiality*, September 2003.

[452] National Institute of Standards and Technology (NIST). Announcing Proposed Withdrawal of Federal Information Processing Standard (FIPS) for the Data Encryption Standard (DES) and Request for Comments. *U.S. Federal Register*, 69(142):44509–44510, July 2004.

[453] National Institute of Standards and Technology (NIST). *NIST Special Publication 800-22: Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, May 2004.

[454] R. M. Needham and M. D. Schroeder. Using encryption for authentication in large networks of computers. *Communications of the ACM*, 21:993–999, 1978.

[455] B. C. Neuman and T. Ts'o. Kerberos: an authentication service for computer networks. *IEEE Communications Magazine*, 32(9):33–38, September 1994.

[456] New European Schemes for Signatures, Integrity and Encryption (NESSIE). NESSIE Security Report, version 2.0. Available from http://www.cryptonessie.org/, 2003.

[457] New European Schemes for Signatures, Integrity and Encryption (NESSIE). Performance of optimized implementations of the NESSIE primitives, version 2.0. Available from http://www.cryptonessie.org/, 2003.

[458] P. Q. Nguyen and I. E. Shparlinski. The insecurity of the Digital Signature Algorithm with partially known nonces. *Journal of Cryptology*, 15(3):151–176, 2002.

[459] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[460] M. Nystrom and B. Kaliski. *RFC 2986, PKCS #10: Certification Request Syntax Specification Version 1.7*. Internet Engineering Task Force, November 2000.

[461] H. Ohta and M. Matsui. *RFC 2994, A Description of the MISTY1 Encryption Algorithm*. Internet Engineering Task Force, November 2000.

[462] Organization for the Advancement of Structured Information Standards. *OASIS XML Common Biometric Format, Committee Specification 1.1*, June 2003.

[463] H. Orman. *RFC 2412, The OAKLEY Key Determination Protocol*. Internet Engineering Task Force, November 1998.

[464] T. Palmer. PKI needs good standards? *Information Security Technical Report*, 8(3):6–13, 2003.

[465] K. G. Paterson and A. Yau. Padding oracle attacks on the ISO CBC mode encryption standard. In T. Okamoto, editor, *Topics in Cryptology — CT-RSA 2004*, volume 2964 of *Lecture Notes in Computer Science*, pages 305–323. Springer-Verlag, 2004.

[466] E. Petrank and C. Rackoff. CBC MAC for real-time data sources. *Journal of Cryptology*, 13:315–338, 2000.

[467] C. P. Pfleeger. *Security in Computing.* Prentice-Hall PTR, 2nd edition, 1997.

[468] D. Pinkas and R. Housley. *RFC 3379, Delegated Path Validation and Delegated Path Discovery Protocol Requirements.* Internet Engineering Task Force, September 2002.

[469] D. Pinkas, N. Pope, and J. Ross. *RFC 3628, Policy Requirements for Time-Stamping Authorities (TSAs).* Internet Engineering Task Force, November 2003.

[470] F. Piper and S. Murphy. *Cryptography: A Very Short Introduction.* Oxford University Press, 2002.

[471] W. Polk, R. Housley, and L. Bassham. *RFC 3279, Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.* Internet Engineering Task Force, April 2002.

[472] G. Poupard and J. Stern. Security analysis of a practical "on the fly" authentication and signature generation. In K. Nyberg, editor, *Advances in Cryptology — Eurocrypt '98*, volume 1403 of *Lecture Notes in Computer Science*, pages 422–436. Springer-Verlag, 1998.

[473] H. Prafullchandra and J. Schaad. *RFC 2875, Diffie-Hellman Proof-of-Possession Algorithms.* Internet Engineering Task Force, July 2000.

[474] B. Preneel, R. Govaerts, and J. Vandewalle. Hash functions based on block ciphers: A synthetic approach. In D. R. Stinson, editor, *Advances in Cryptology – Crypto '93*, volume 773 of *Lecture Notes in Computer Science*, pages 368–378. Springer-Verlag, 1993.

[475] B. Preneel, V. Rijmen, and P. C. van Oorschot. A security analysis of the Message Authenticator Algorithm (MAA). *European Transactions on Telecommunications*, 8:455–470, 1997.

[476] B. Preneel and P. C. van Oorschot. MDx-MAC and building fast MACs from hash functions. In D. Coppersmith, editor, *Advances in Cryptology — Crypto '95*, volume 963 of *Lecture Notes in Computer Science*, pages 1–14. Springer-Verlag, 1995.

[477] B. Preneel and P. C. van Oorschot. A key recovery attack on the ANSI X9.19 retail MAC. *Electronics Letters*, **32**:1568–1569, 1996.

[478] M. O. Rabin. Digitalized signatures. In R. Lipton and R. DeMillo, editors, *Foundations of Secure Computation*, pages 216–231. Academic Press, 1978.

[479] M. O. Rabin. Probabilistic algorithm for testing primality. *Journal of Number Theory*, 12:128–138, 1980.

[480] W. Rankl and W. Effing. *Smart Card Handbook*. John Wiley and Sons Ltd., 3rd edition, 2003.

[481] E. Rescorla. *RFC 2631: Diffie-Hellman Key Agreement Method*. Internet Engineering Task Force, June 1999.

[482] R. L. Rivest. *RFC 1320, The MD4 message-digest algorithm*. Internet Engineering Task Force, April 1992.

[483] R. L. Rivest. *RFC 1321, The MD5 message-digest algorithm*. Internet Engineering Task Force, April 1992.

[484] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21:120–126, 1978.

[485] M. Roe. *Non-repudiation and evidence*. PhD thesis, University of Cambridge, 1997.

[486] P. Rogaway, M. Bellare, and J. Black. OCB: A block-cipher mode of operation for efficient authenticated encryption. *ACM Transactions on Information and System Security*, 6:365–403, 2003.

[487] P. Rogaway, M. Bellare, J. Black, and T. Krovetz. OCB: A block-cipher mode of operation for efficient authenticated encryption. In *Proceedings of the Eighth ACM Conference on Computer and Communications Security (CCS-8)*, pages 196–205. ACM Press, 2001.

[488] P. Rogaway and T. Shrimpton. Cryptographic hash-function basics: Definitions, implications, and separations for preimage resistance, second-preimage resistance, and collision resistance. In B. Roy and W. Meier, editors, *Proceedings of the 11th Workshop on Fast Software Encryption (FSE 2004)*, volume 3017 of *Lecture Notes in Computer Science*, pages 371–388. Springer-Verlag, 2004.

[489] P. Rogaway and D. Wagner. A critique of CCM. Available from `http://www.cs.ucdavis.edu/~rogaway/papers/`, 2003.

[490] N. Rogier and P. Chauvaud. The compression function of MD2 is not collision free. In *2nd Workshop on Selected Areas of Cryptography (SAC '95)*, 1995.

[491] J. Rosenoer. *Cyberlaw: The law of the Internet*. Springer-Verlag, 1997.

[492] RSA Laboratories. *PKCS #11 v2.11: Cryptographic Token Interface Standard, Revision 1*, November 2001.

[493] P. Ryan, S. Schneider, M. Goldsmith, G. Lowe, and B. Roscoe. *The modelling and analysis of security protocols: The CSP approach.* Addison-Wesley, 2000.

[494] S. Santesson, W. Polk, P. Barzin, and M. Nystrom. *RFC 3039, Internet X.509 Public Key Infrastructure: Qualified Certificates Profile.* Internet Engineering Task Force, January 2001.

[495] J. Schaad and R. Housley. *RFC 3394, Advanced Encryption Standard (AES) Key Wrap Algorithm.* Internet Engineering Task Force, September 2002.

[496] B. Schneier. *Applied Cryptography.* John Wiley and Sons, Inc., 2nd edition, 1996.

[497] C. P. Schnorr. Efficient identification and signatures for smart cards. In G. Brassard, editor, *Advances in Cryptology — Crypto '89*, volume 435 of *Lecture Notes in Computer Science*, pages 239–252. Springer-Verlag, 1990.

[498] A. Shamir. How to share a secret. *Communications of the ACM*, 22:612–613, 1979.

[499] A. Shamir. Identity-based cryptosystems and signature schemes. In G. R. Blakley and D. Chaum, editors, *Advances in Cryptology – Crypto '84*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer-Verlag, 1984.

[500] C. E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27:379–423, 623–656, 1948.

[501] C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28:656–715, 1949.

[502] J. Shawe-Taylor. Generating strong primes. *Electronics Letters*, 22(16):875–877, 1986.

[503] P. W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings of the IEEE 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.

[504] V. Shoup. Using hash functions as a hedge against chosen ciphertext attack. In B. Preneel, editor, *Advances in Cryptology – Eurocrypt 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 275–288. Springer-Verlag, 2000.

[505] G. J. Simmons, editor. *Contemporary Cryptology: The Science of Information Integrity.* IEEE Press, 1992.

[506] F. Stajano. *Security for Ubiquitous Computing*. John Wiley and Sons Ltd., 2002.

[507] F. Stajano and R. Anderson. The resurrecting duckling: Security issues for ad-hoc wireless networks. In B. Christianson, B. Crispo, J. A. Malcolm, and M. Roe, editors, *Security Protocols, 7th International Workshop*, volume 1976 of *Lecture Notes in Computer Science*, pages 172–194. Springer-Verlag, 2000.

[508] W. Stallings. *Cryptography and Network Security*. Prentice Hall, 2003.

[509] W. Stallings. *Data and Computer Communications*. Prentice Hall, 7th edition, 2004.

[510] Standards for Efficient Cryptography Group. *SEC 1: Elliptic Curve Cryptography*, September 2000.

[511] Standards for Efficient Cryptography Group. *SEC 2: Recommended Elliptic Curve Domain Parameters*, September 2000.

[512] J. G. Steiner, C. Neuman, and J. I. Schiller. Kerberos: an authentication service for open network systems. In *Proceedings: Usenix Association, Winter Conference 1988*, pages 191–202. USENIX Association, Berkeley, California, February 1988.

[513] D. R. Stinson. *Cryptography: Theory and Practice*. CRC Press, 1995.

[514] Telecommunication Technology Association, Korea. *TTAS.KO-12.0004, 128-bit symmetric block cipher (SEED)*, September 1999.

[515] R. Temple and J. Regnault. *Internet and wireless security*. Institute of Electrical Engineers, 2002.

[516] Utah State Legislature. *Utah Digital Signature Act*, 1996. Available from `http://www.le.state.ut.us/~code/TITLE46/TITLE46.htm`.

[517] S. Vaudenay. Security flaws induced by CBC padding — Applications to SSL, IPSEC, WTLS ... In L. R. Knudsen, editor, *Advances in Cryptology — Eurocrypt 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 534–545. Springer-Verlag, 2002.

[518] Xiaoyun Wang, Dengguo Feng, Xuejia Lai, and Hongbo Yu. Collisions for hash functions MD4, MD5, HAVAL-128 and RIPEMD. Available from `http://eprint.iacr.org/2004/199/`, 2004.

[519] D. Watanabe, A. Biryukov, and C. De Cannière. A distinguishing attack of SNOW 2.0 with linear masking method. In M. Matsui and R. Zuccherato, editors, *Selected Areas in Cryptography, 10th Annual*

International Workshop, SAC 2003, volume 3006 of *Lecture Notes in Computer Science*, pages 222–233. Springer-Verlag, Berlin, 2004.

[520] D. Watanabe, S. Furuya, H. Yoshida, K. Takaragi, and B. Preneel. A new keystream generator MUGI. In J. Daemen and V. Rijmen, editors, *Fast Software Encryption, 9th International Workshop, FSE 2002*, volume 2365 of *Lecture Notes in Computer Science*, pages 179–194. Springer-Verlag, Berlin, 2002.

[521] D. Welsh. *Codes and Cryptography*. Oxford University Press, 1988.

[522] D. Whiting, R. Housley, and N. Ferguson. *RFC 3610, Counter with CBC-MAC (CCM)*. Internet Engineering Task Force, September 2003.

[523] M. J. Wiener. Efficient DES key search. Technical Report TR–244, Carleton University, 1993. Available from http://www.ja.net/CERT/Wiener/des_key_search.ps.

[524] J. Wray. *RFC 1509, Generic Security Service API : C-bindings*. Internet Engineering Task Force, September 1993.

[525] J. Wray. *RFC 2744, Generic Security Service API Version 2: C-bindings*. Internet Engineering Task Force, January 2000.

[526] A. C. Yao. Theory and applications of trapdoor functions. In *27th IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 80–91, 1982.

[527] W. Yeong, T. Howes, and S. Kille. *RFC 1777, Lightweight Directory Access Protocol*. Internet Engineering Task Force, March 1995.

[528] Y. Zheng. Digital signcryption or how to achieve cost(signature & encryption) << cost(signature) + cost(encryption). In B. Kaliski, editor, *Advances in Cryptology – Crypto '97*, volume 1294 of *Lecture Notes in Computer Science*, pages 165–179. Springer-Verlag, 1997.

[529] J. Zhou. *Non-repudiation*. PhD thesis, Royal Holloway, University of London, 1997.

[530] J. Zhou. *Non-repudiation in electronic commerce*. Artech House, 2001.

[531] J. Zhou, R. Deng, and F. Bao. Evolution of fair non-repudiation with TTP. In J. Pieprzyk, R. Safavi-Naini, and J. Seberry, editors, *Information Security and Privacy, 4th Australasian Conference, ACISP '99*, volume 1587 of *Lecture Notes in Computer Science*, pages 258–269. Springer-Verlag, 1999.

[532] J. Zhou and D. Gollmann. A fair non-repudiation protocol. In *Proceedings: 1996 IEEE Symposium on Security and Privacy*, pages 55–61. IEEE Computer Society Press, 1996.

[533] E. D. Zwicky, D. B. Chapman, and S. Cooper. *Building Internet Firewalls*. O'Reilly, 2nd edition, 2000.